AFRL-RI-RS-TR-2015-262

USING MATHEMATICS TO MAKE COMPUTING ON ENCRYPTED DATA SECURE AND PRACTICAL

UNIVERSITY OF CALIFORNIA, IRVINE

DECEMBER 2015

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2015-262 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /
CARL THOMAS
Work Unit Manager

/ S /
MARK LINDERMAN
Technical Advisor, Computing & Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
DECEMBER 2015	FINAL TECHNICAL REPORT	DEC 2012 – JUN 2015

4. TITLE AND SUBTITLE

USING MATHEMATICS TO MAKE COMPUTING ON ENCRYPTED DATA SECURE AND PRACTICAL

5a. CONTRACT NUMBER
FA8750-13-2-0054

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62303E

6. AUTHOR(S)

Alice Silverberg and Hendrik Lenstra

5d. PROJECT NUMBER
PROC

5e. TASK NUMBER
E2

5f. WORK UNIT NUMBER
UC

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of California, Irvine
5171 California Ave, Suite 150
Irvine, CA 92617-3067

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Advanced Research ProjectsAgency
675 North Randolph St
Arlington, VA 22203-2114

Air Force Research Laboratory/RITA
525 Brooks Road
Rome, NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2015-262

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Provides a deterministic polynomial-time algorithm that decides whether a lattice with enough symmetry has an orthonormal basis, and finds one if it does.

15. SUBJECT TERMS
Fully Homomorphic Encryption (FHE), Lenkstra-Lenkstra-Lovasz (LLL) lattice basis reduction algorithm, G-Lattice, Cryptography, Security, Gentry-Szydlo Algorithm, Ring-LWE

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**CARL THOMAS**
U	U	U	UU	84	19b. TELEPHONE NUMBER (*Include area code*) **315-330-2600**

Table of Contents

Section Page

1. Summary

In order to make computing on encrypted data more practical to use and more secure from attack, it is necessary to discover, develop, and understand the mathematics on which it is based and the mathematics that can be used to attack it. The security of homomorphic encryption schemes is based on the presumed difficulty of mathematics problems about lattices. Discovering and fully exploring algorithms to solve these mathematical problems allow computing on encrypted data to be performed with confidence, knowing that its cryptographic security is based on sound mathematical foundations.

Hendrik Lenstra and Alice Silverberg discovered and developed algorithms to solve some lattices problems under suitable conditions, and investigated the mathematical foundations of these algorithms. A primary method of attack on homomorphic encryption schemes consists of lattice algorithms performed on ideal lattices, which are lattices with a certain type of algebraic structure. Any structure or symmetry is potentially susceptible to exploitation and attack. The work performed here gives algorithms for lattice problems for lattices that have symmetry. Recommendations are that the mathematical foundations of lattices with symmetry be further developed, in order to quantify the security of lattice-based cryptography, including especially the security of homomorphic encryption schemes.

2. Introduction

In encryption schemes, one party encrypts a plaintext message to obtain a ciphertext. The other party decrypts the ciphertext to recover the plaintext. In Fully Homomorphic Encryption (FHE), parties that do not know the plaintext data can perform computations on it by performing computations on the corresponding ciphertexts.

The security of essentially all currently known FHE schemes is based on the presumed difficulty of some lattice problem, such as finding an approximately shortest (non-zero) vector in a high dimensional lattice. The primary known attacks on FHE schemes are variants of the LLL lattice basis reduction algorithm [7], originally due to Lenstra, Lenstra, and Lovász.

A number of Fully Homomorphic Encryption schemes use ideal lattices rather than arbitrary lattices, including Gentry's first FHE scheme [3]. Fully Homomorphic Encryption is performed more efficiently with ideal lattices than with general lattices. However, ideal lattices are very special lattices, with much structure ("symmetries") that has the potential to be exploited, and it might turn out to be the case that lattice attacks are easier for ideal lattices than for generic lattices.

In §7 of [5], Gentry and Szydlo introduced some powerful new ideas that combined in a clever way lattice basis reduction and number theory. They used these ideas to cryptanalyze NTRU (NTRUEncrypt Public Key Cryptosystem) Signatures. The recent interest in Fully Homomorphic Encryption and in the candidate multilinear maps of Garg-Gentry-Halevi [2] have renewed the interest in the Gentry-Szydlo results from [5].

In his PhD thesis [4], Gentry mentions that the Gentry-Szydlo attack on NTRU signatures can be used to attack principal ideal lattices in the ring $\mathbb{Z}[X]/(X^n - 1)$, if the lattice has an orthonormal basis.

The algorithm of Gentry and Szydlo can be viewed as a way to find an orthonormal basis (if one exists) for an ideal lattice. Determining whether a lattice has an orthonormal basis is in general a difficult algorithmic problem. The main results reported here show that this problem is easier when the lattice has many symmetries. We also put the Gentry-Szydlo algorithm into a mathematical framework, and show that it is part of a general theory of "lattices with symmetry". This sheds new light on the Gentry-Szydlo algorithm, and the ideas should be applicable to a range of questions in cryptography.

The new algorithm of Lenstra and Silverberg runs in deterministic polynomial time, whereas the Gentry-Szydlo algorithm in §7 of [5] was based on heuristic assumptions. Also, the Lenstra-Silverberg setting is more general (it applies to arbitrary finite abelian groups, whereas [5] considered only cyclic groups of odd prime order), thereby covering other cases of potential cryptographic interest.

The main results are joint work with Hendrik Lenstra [9, 10, 11, 12] (see appendix). In [13] we give an exposition of FHE for a mathematical audience (see appendix), which gives some useful background. See [1] for mathematical background in commutative algebra.

3. Methods, Assumptions, and Procedures

The techniques involve algorithmic algebraic number theory, analytic number theory, commutative algebra, and lattice basis reduction. Let $\mathbb{Z}$ denote the ring of integers. Let $\mathbb{Z}[X]$ denote the ring of polynomials in one variable X with integer coefficients.

3.1. **The Gentry-Szydlo Algorithm.** The Gentry-Szydlo algorithm in §7 of [5] finds a generator v of a principal ideal in the quotient ring $\mathbb{Z}[X]/(X^n - 1)$, given $v\overline{v}$ and a $\mathbb{Z}$-basis for the ideal. Here, n is an odd prime number, and for

$$v = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$$

its "reversal" is defined to be

$$\overline{v} = a_0 + a_{n-1} X + \ldots + a_1 X^{n-1}.$$

The information $v\overline{v}$ is the crucial "hint" that gives enough structure (i.e., "symmetry") to recover the generator v of the principal ideal.

A brief sketch of the Gentry-Szydlo algorithm in §7 of [5] is the following:

(i) Choose auxiliary large prime numbers P, P' such that

$$\gcd(P - 1, P' - 1) = 2n.$$

(ii) Use polynomial chains and the LLL algorithm [7] to compute v^{P-1} and $v^{P'-1}$ modulo other auxiliary prime numbers.

(iii) Use the Euclidean algorithm to compute v^{2n}.

(iv) Recover v.

In §7 of [5], taking powers of an ideal in the ring $R = \mathbb{Z}[X]/(X^n - 1)$ required complicated bookkeeping, via polynomial chains and lattice basis reduction to avoid coefficient blow-up. When one multiplies ideals, coefficients (with respect to any $\mathbb{Z}$-basis) grow quickly, because of the way the ideals are embedded in the ring. Where Gentry-Szydlo use the *ideal* structure of ideal lattices, Lenstra and Silverberg [9, 11] do away with this, by using only the *module* structure of the ideal, rather than its ideal structure. More precisely, an ideal in a commutative ring R is the same as an R-module M along with an embedding $M \hookrightarrow R$ of R-modules. While Gentry and Szydlo use the embedding, Lenstra and Silverberg observe that one can avoid coefficient blow-up by using the module structure of M but not the actual embedding. Lenstra and Silverberg also replace ideal multiplication with tensor products of lattices. By tensoring abstract modules rather than multiplying ideals, we avoid the need to keep track of embeddings into the ring and large coefficients. We introduce a graded tensor algebra that replaces Gentry's and Szydlo's polynomial chains.

More specifically, where Gentry and Szydlo use polynomial chains:

$$v_0^{k_{r-1}} v_0^2 \overline{v}_1 \ , \ v_0^{k_{r-2}} v_1^2 \overline{v}_2 \ , \ \ldots \ , \ v_0^{k_0} v_{r-1}^2 \overline{v}_r$$

$$\text{and} \quad v_0 \overline{v}_0 \ , \ v_1 \overline{v}_1 \ , \ \ldots \ , \ v_{r-1} \overline{v}_{r-1},$$

in the new papers [9, 11] a graded tensor algebra is used instead:

$$\ldots \oplus \overline{L}^{\otimes 2} \oplus \overline{L} \oplus L^0 \oplus L \oplus L^{\otimes 2} \oplus L^{\otimes 3} \oplus \ldots$$

where L is the ideal lattice, and $\overline{L}$ and L^0 are suitably defined (below).

In addition, where Gentry and Szydlo [5] use auxiliary large prime numbers P and P', Lenstra and Silverberg [9, 11] use auxiliary large prime powers. An analytic number theory result then allows us to replace the heuristic polynomial-time algorithm in [5] with a more efficient provably deterministic polynomial time-algorithm.

3.2. **Lattices.** See [8] for background on lattices.

Definition 1. A **lattice** is a finitely generated abelian group L with a map

$$L \times L \to \mathbb{Z}, \qquad (x, y) \mapsto \langle x, y \rangle$$

that is

- bilinear, i.e.,
$$\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$$
and
$$\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$$
for all $x, y, z \in L$,
- symmetric, i.e.,
$$\langle x, y \rangle = \langle y, x \rangle$$
for all $x, y \in L$, and
- positive definite, i.e.,
$$\langle x, x \rangle > 0$$
if $0 \neq x \in L$.

Example 2. The **standard lattice** of rank n is $\mathbb{Z}^n$ with inner product $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$.

Definition 3. An **isomorphism** of lattices L and M is a group isomorphism

$$\varphi : L \xrightarrow{\sim} M$$

that respects the lattice structures, i.e.,

$$\langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$$

for all $x, y \in L$. If such a map φ exists, then L and M are **isomorphic** lattices. An **automorphism** of a lattice L is an isomorphism from L to itself. The set of automorphisms of L is a finite group $\mathrm{Aut}(L)$ that contains -1.

For a lattice, having an orthonormal basis is the same as being isomorphic to the standard lattice of the same rank.

3.3. **G-lattices.** Fix a finite abelian group G and an element u in G of order 2.

Definition 4. A *G-lattice* is a lattice with a G-action, with u acting as -1. In other words, a G-lattice is a lattice L with a group homomorphism

$$f : G \to \mathrm{Aut}(L)$$

such that

$$f(u) = -1.$$

For $\sigma \in G$ and $x \in L$ let

$$\sigma x = f(\sigma)(x).$$

Definition 5. If L and M are G-lattices, then a **G-isomorphism** is an isomorphism $\varphi : L \xrightarrow{\sim} M$ of lattices that respects the G-actions, i.e.,

$$\varphi(\sigma x) = \sigma\varphi(x)$$

for all $x \in L$ and $\sigma \in G$.

Let

$$\mathbb{Z}[G] := \{\sum_{\sigma\in G} a_\sigma \sigma : a_\sigma \in \mathbb{Z}\}.$$

Definition 6. The *standard G-lattice* $\mathbb{Z}\langle G\rangle$ is $\mathbb{Z}[G]/(u+1)$ with lattice structure defined by

$$\langle x, y\rangle = t(x\overline{y}),$$

where

$$\overline{\sum_{\sigma\in G} a_\sigma \sigma} := \sum_{\sigma\in G} a_\sigma \sigma^{-1}$$

and

$$t(\sum_{\sigma\in G} a_\sigma \sigma) := a_1 - a_u \in \mathbb{Z}.$$

Let

$$n = \frac{|G|}{2}.$$

Then $\mathbb{Z}\langle G\rangle$ is a G-lattice of rank n. As lattices, $\mathbb{Z}\langle G\rangle$ is isomorphic to $\mathbb{Z}^n$. Further,

$$\mathbb{Z}\langle G\rangle = \{\sum_{\sigma\in S} a_\sigma \sigma : a_\sigma \in \mathbb{Z}\}$$

where S is a set of coset representatives of the quotient group $G/\langle u\rangle$ (i.e., $\#S = n$ and G is the disjoint union of S and uS).

Example 7. If $G = \langle u\rangle \times \mathbb{Z}/n\mathbb{Z}$, then

$$\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[\mathbb{Z}/n\mathbb{Z}] \cong \mathbb{Z}[X]/(X^n - 1).$$

Example 8. If G is cyclic, then

$$\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[X]/(X^n + 1).$$

Example 9. If G is cyclic of order 2^r, and ζ_{2^r} is a primitive 2^r-th root of unity, then

$$\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[\zeta_{2^r}].$$

Definition 10. A G-lattice L is *invertible* if L is a unimodular lattice and there is a $\mathbb{Z}\langle G\rangle$-module M such that $L \otimes_{\mathbb{Z}\langle G\rangle} M$ and $\mathbb{Z}\langle G\rangle$ are isomorphic as $\mathbb{Z}\langle G\rangle$-modules.

Definition 11. If L is a G-lattice, then the G-lattice $\overline{L}$ is a lattice equipped with a lattice isomorphism $L \xrightarrow{\sim} \overline{L}$, $x \mapsto \overline{x}$ and a group homomorphism $G \to \mathrm{Aut}(\overline{L})$ defined by

$$\sigma\overline{x} = \overline{\sigma^{-1}x}$$

for all $\sigma \in G$ and $x \in L$.

3.4. **Auxiliary prime powers.**

Definition 12. The **exponent** of a group H is the least positive integer k such that $\sigma^k = 1$ for all $\sigma \in H$.

The exponent of a group H divides the order $|H|$ of H and has the same prime factors as $|H|$.

Definition 13. Let k be the exponent of the group G and let $k(m)$ be the exponent of the group $(\mathbb{Z}\langle G\rangle/(m))^*$.

We replace the Gentry-Szydlo auxiliary prime numbers P and P' such that

$$\gcd(P-1, P'-1) = 2n$$

with auxiliary prime powers ℓ and m such that

$$\gcd(k(\ell), k(m)) = k.$$

While the Gentry-Szydlo prime numbers P and P' are found with at best a probabilistic algorithm, the prime powers ℓ and m used in [9, 11] can be found with a deterministic algorithm that runs in polynomial time, thanks to a result from analytic number theory:

Theorem 14 (Heath-Brown [6])**.** *There is an effective positive constant c such that if a and t are relatively prime positive integers, then the smallest prime number p such that $p \equiv a \bmod t$ is at most $ct^{5.5}$.*

The ring elements that Gentry and Szydlo work with were required to not be zero divisors modulo P, P', and other auxiliary prime numbers. We require no analogous condition on ℓ and m.

Along the way towards formulating and proving our main algorithms, we prove and use:

Theorem 15. *If L is an invertible G-lattice, then the map*

$$\{G\text{-isomorphisms } \mathbb{Z}\langle G\rangle \to L\} \to \{ \text{ vectors of } L \text{ of length } 1\}$$

that sends f to $f(1)$ is bijective.

4. Results and Discussion

For large ranks, there is no good algorithm that decides whether a given lattice has an orthonormal basis (i.e., is isomorphic to a standard lattice $\mathbb{Z}^n$). Lenstra and Silverberg construct a provably deterministic polynomial-time algorithm that decides whether a given lattice with sufficiently many symmetries has an orthonormal basis, and finds one if it does. It is based on the algorithm of Gentry and Szydlo in §7 of [5].

More precisely, we give a deterministic polynomial time algorithm that decides whether a G-lattice is G-isomorphic to the standard G-lattice $\mathbb{Z}\langle G\rangle$, and if it is, exhibits such an isomorphism.

Theorem 16 (Lenstra and Silverberg, [9, 11])**.** *There is a deterministic polynomial time algorithm that, given a finite abelian group G, an element u in G of order 2, and a G-lattice L, decides whether L and $\mathbb{Z}\langle G\rangle$ are G-isomorphic, and if they are, exhibits a G-isomorphism.*

Recall the definitions of the exponents k and $k(m)$ from Definition 13.

Here is a sketch of the main algorithm:

(i) Check whether L is invertible.
(ii) Produce large prime powers ℓ and m such that $\gcd(k(\ell), k(m)) = k$.
(iii) Compute $e_{\ell m} \in L$ that generates $L/\ell mL$ as a $\mathbb{Z}\langle G\rangle/(\ell m)$-module.
(iv) Find a vector of length 1 in $L^{\otimes k(m)}$, if one exists.
(v) Find a vector of length 1 in $L^{\otimes k}$, if one exists.
(vi) Find a vector e of length 1 in L, if one exists.
(vii) The desired isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ is $x \mapsto xe$.

Since one can get an orthonormal basis for the standard G-lattice from half the group elements, it follows that the algorithm decides whether a G-lattice has an orthonormal basis, and finds one if it does.

Even more, we can determine whether two invertible G-lattices are G-isomorphic, and if they are, find such an isomorphism, as in the following result.

Corollary 17 (Lenstra and Silverberg, [11])**.** *There is a deterministic polynomial time algorithm that, given a finite abelian group G, an element u in G of order 2, and two invertible G-lattices L and M, determines whether there is a G-isomorphism $M \xrightarrow{\sim} L$, and if so, computes one.*

We next explain how to recover the Gentry-Szydlo algorithm in §7 of [5] from the above algorithm. Recall that the Gentry-Szydlo algorithm finds a generator v of a principal ideal I of $\mathbb{Z}[X]/(X^n - 1)$ (with n an odd prime number), given $v\overline{v}$ and a $\mathbb{Z}$-basis for I. Let G be a cyclic group of order $2n$. Then $\mathbb{Z}\langle G\rangle = \mathbb{Z}[X]/(X^n - 1)$. Make I into a G-lattice with lattice structure defined by

$$\langle x, y\rangle = t(x\overline{y}/v\overline{v}).$$

The above algorithm produces a G-isomorphism

$$\varphi : \mathbb{Z}\langle G\rangle \xrightarrow{\sim} I$$

in polynomial time, and thus gives a generator $v = \varphi(1)$ of the ideal I in polynomial time.

On the way, we give in [10] a deterministic polynomial-time algorithm that determines whether a finite module over a finite commutative ring is cyclic, and if it is, outputs a generator.

Definition 18. If R is a commutative ring, then an R-module M is cyclic if there exists $y \in M$ such that $M = Ry$.

Theorem 19. *There is a deterministic polynomial-time algorithm that, given a finite commutative ring R and a finite R-module M, decides whether there exists $y \in M$ such that $M = Ry$, and if there is, finds such a y.*

We also give [12] a deterministic polynomial-time algorithm that, given an order, determines a set of generators for the group of roots of unity in the order.

Definition 20. An **order** is a commutative ring A whose additive group is isomorphic to $\mathbb{Z}^n$ for some non-negative integer n.

Definition 21. If R is a commutative ring, then we write

$$\mu(R) = \{z \in R : z^r = 1 \text{ for some positive integer } r\},$$

the group of *roots of unity* in R.

The group $\mu(R)$ is a subgroup of the group R^* of invertible elements of R.

Theorem 22. *There is a deterministic polynomial-time algorithm that, given an order A, produces a set of generators S of $\mu(A)$, as well as a set of defining relations for S.*

5. Conclusions

We give a deterministic polynomial-time algorithm that decides whether a lattice with enough symmetry has an orthonormal basis, and finds one if it does. More precisely, we give a deterministic polynomial-time algorithm that, given a finite abelian group G, an element u in G of order 2, and a G-lattice L, decides whether L and $\mathbb{Z}\langle G\rangle$ are G-isomorphic, and if they are, exhibits a G-isomorphism. We also give a deterministic polynomial time algorithm that, given a finite abelian group G, an element u in G of order 2, and two invertible G-lattices L and M, determines whether there is a G-isomorphism $M \xrightarrow{\sim} L$, and if so, computes one.

These results generalize the algorithm in §7 of the paper [5] of Gentry and Szydlo. Our algorithms are deterministic algorithms that run in (provably) polynomial time, whereas the Gentry-Szydlo algorithm was based on heuristic assumptions. The new mathematics that we developed sheds light on what the Gentry-Szydlo algorithm does and why it works. Our setting is more general, covering more cases of potential cryptographic interest. We remark that the Gentry-Szydlo and Lenstra-Silverberg algorithms are not known to weaken the security of cryptosystems whose security is based on the presumed difficulty of the Ring-LWE Problem.

6. Recommendations

In order to give convincing evidence that methods for computing on encrypted data are cryptographically secure, it is important to discover, develop, and understand the mathematical foundations on which these methods rely. This will enable the construction of more efficient and secure systems, and will give reliable information and confidence as to which systems are secure. Recent proposals for secure computing on encrypted data make use of lattices that have some symmetry. Therefore, the primary recommendation is that the mathematical foundations of lattices with symmetry be discovered and developed. An additional recommendation is that the security of homomorphic encryption schemes based on ideal lattices be quantified, in order to give confidence in the security of such schemes and in order to be able to effectively compare different schemes.

Bibliography

[1] M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, MA, 1969.

[2] S. Garg, C. Gentry, and S. Halevi, *Candidate multilinear maps from ideal lattices*, Advances in Cryptology—EUROCRYPT 2013, Lect. Notes in Comp. Sci. **7881**, Springer, 2013, 1–17.

[3] C. Gentry, *Fully homomorphic encryption using ideal lattices*, in Proceedings of the 41st ACM Symposium on Theory of Computing—STOC 2009, ACM, New York (2009), 169–178.

[4] C. Gentry, *A fully homomorphic encryption scheme*, Stanford University PhD thesis, 2009, `http://crypto.stanford.edu/craig/craig-thesis.pdf`.

[5] C. Gentry and M. Szydlo, *Cryptanalysis of the revised NTRU signature scheme*, Advances in Cryptology—EUROCRYPT 2002, Lect. Notes in Comp. Sci. **2332**, Springer, Berlin, 2002, 299-320, full version at `http://www.szydlo.com/ntru-revised-full02.pdf`.

[6] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), 265–338.

[7] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[8] H. W. Lenstra, Jr., *Lattices*, in Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press, Cambridge, 2008, 127–181.

[9] H. W. Lenstra, Jr. and A. Silverberg, *Revisiting the Gentry-Szydlo Algorithm*, in Advances in Cryptology—CRYPTO 2014, Lect. Notes in Comp. Sci. **8616**, Springer, Berlin, 2014, 280–296.

[10] H. W. Lenstra, Jr. and A. Silverberg, *Determining cyclicity of finite modules*, to appear in Journal of Symbolic Computation (2015).

[11] H. W. Lenstra, Jr. and A. Silverberg, *Lattices with symmetry*, submitted.

[12] H. W. Lenstra, Jr. and A. Silverberg, *Roots of unity in orders*, in preparation.

[13] A. Silverberg, *Fully Homomorphic Encryption for Mathematicians*, in WIN 2: Research Directions in Number Theory, Contemp. Math. **606**, American Mathematical Society and Centre de Recherches Mathématiques (2013), 111–123.

List of Symbols, Abbreviations, and Acronyms

FHE Fully Homomorphic Encryption

LLL Lenstra-Lenstra-Lovász lattice basis reduction algorithm

$\mathbb{Z}$ the integers

$\mathbb{Z}[X]$ the set of polynomials in one variable X with integer coefficients

$|G|$ the number of elements in a set G

Appendix consisting of papers written under this grant

This appendix consists of the following papers, which were Contracted Fundamental Research (CFR) and did not require approval:

- Fully Homomorphic Encryption for Mathematicians,
  by A. Silverberg,
  in WIN 2: Research Directions in Number Theory,
  Contemporary Mathematics **606**,
  American Mathematical Society and Centre de Recherches Mathématiques (2013), 111–123.

- Revisiting the Gentry-Szydlo Algorithm,
  by H. W. Lenstra Jr. and A. Silverberg,
  in Advances in Cryptology—CRYPTO 2014,
  Lecture Notes in Computer Science **8616** (2014),
  Springer, 280–296.

- Determining cyclicity of finite modules,
  by H. W. Lenstra Jr. and A. Silverberg,
  to appear in Journal of Symbolic Computation (2015).

- Lattices with symmetry,
  by H. W. Lenstra Jr. and A. Silverberg.

Fully Homomorphic Encryption for Mathematicians

Alice Silverberg

Abstract. We give an introduction to Fully Homomorphic Encryption for mathematicians. Fully Homomorphic Encryption allows untrusted parties to take encrypted data $\mathrm{Enc}(m_1), \ldots, \mathrm{Enc}(m_t)$ and any efficiently computable function f, and compute an encryption of $f(m_1, \ldots, m_t)$, without knowing or learning the decryption key or the raw data $m_1, \ldots, m_t$. The problem of how to do this was recently solved by Craig Gentry, using ideas from algebraic number theory and the geometry of numbers. In this paper we discuss some of the history and background, give examples of Fully Homomorphic Encryption schemes, and discuss the hard mathematical problems on which the cryptographic security is based.

1. Introduction

Fully Homomorphic Encryption (FHE) has been referred to as a "holy grail" of cryptography. Craig Gentry's recent solution to the problem, while not efficient enough to be practical, was considered to be a major breakthrough. Since then, much progress has been made in the direction of finding efficient Fully Homomorphic Encryption schemes.

In this paper we will give a brief introduction to FHE for mathematicians. We will give some of the history and major ideas, we will present some examples of FHE schemes, and we will mention a variety of security assumptions on which FHE schemes have been based. The intended audience is mathematicians at the graduate level or beyond (especially number theorists) who do not necessarily have any background in

This material is based on research sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750-13-2-0054. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

The work was also supported by the National Science Foundation under grant CNS-0831004.

Thanks go to Hendrik Lenstra for helpful conversations about Fully Homomorphic Encryption, and to Lily Khadjavi, Zvika Brakerski, Chris Peikert, and Steven Galbraith for very helpful comments on earlier versions of the paper.

cryptography. The paper is mostly a survey, though §4.3 gives a number theory proof that does not seem to be in the cryptography literature.

In encryption schemes, Bob encrypts a plaintext message to obtain a ciphertext. Alice decrypts the ciphertext to recover the plaintext. In Fully Homomorphic Encryption, parties that do not know the plaintext data can perform computations on it by performing computations on the corresponding ciphertexts.

A major application of FHE is to cloud computing. Alice can store her data in "the cloud", for example, on remote servers that she accesses via the Internet. The cloud has more storage capabilities and computing power than does Alice, so when Alice needs computations to be done on her data, she would like those computations to be done by the cloud. However, Alice doesn't trust the cloud. Her data might be sensitive (for example, Alice might be a hospital and the data might be patients' medical records), and Alice would like the cloud to know as little as possible about her data, and about the results of the computations. So Alice sends encrypted data to the cloud, which can perform arithmetic operations on it without learning anything about the original raw data, by performing operations on the encrypted data.

Fully Homomorphic Encryption can be used to query a search engine, without revealing what is being searched for (here, the search engine is doing the computations on encryptions of information that it doesn't know).

More precisely, FHE has the following property (in its simplest form). Say that ciphertexts c_i decrypt to plaintexts m_i, i.e., $\text{Decrypt}(c_i) = m_i$, where the m_i's and c_i's are elements of some ring (with two operations, addition and multiplication). In FHE one has

$$\text{Decrypt}(c_1 + c_2) = m_1 + m_2, \qquad \text{Decrypt}(c_1 \cdot c_2) = m_1 \cdot m_2.$$

In other words, decryption is doubly homomorphic, i.e., homomorphic with respect to the two operations addition and multiplication.

Being fully homomorphic means that whenever f is a function composed of (finitely many) additions and multiplications in the ring, then

$$\text{Decrypt}(f(c_1, \ldots, c_t)) = f(m_1, \ldots, m_t).$$

If the cloud (or an adversary) can efficiently compute $f(c_1, \ldots, c_t)$ from ciphertexts $c_1, \ldots, c_t$, without learning any information about the corresponding plaintexts $m_1, \ldots, m_t$, then the system is efficient and secure.

Another requirement for FHE is that the ciphertext sizes remain bounded, independent of the function f; this is known as the "compact ciphertexts" requirement.

(Depending on the FHE system, the messages and ciphertexts could in fact lie in different rings, and multiplication might be accomplished using a tensoring operation, as in [**Br**].)

Fully Homomorphic Encryption schemes can be either public key (where the encryptor knows the decryptor's public key but not her private key) or symmetric key (where the encryptor and decryptor share a key that is used for both encryption and decryption).

In Section 2 we briefly give some history and background. In Sections 3, 4, and 5 we give some (somewhat) homomorphic encryption schemes, to illustrate a variety of techniques and security assumptions.

See [**V2**] for an excellent recent survey article. See also [**H**] for a good explanation of FHE for a general audience.

As usual, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the integers, rational numbers, real numbers, and complex numbers, respectively, and $\mathbb{F}_q$ denotes the finite field with q elements.

2. Some history and background

2.1. Early history. In 1978, shortly after the invention of the RSA cryptosystem, Rivest, Adleman, and Dertouzos [**RAD**] came up with the idea of fully homomorphic encryption, which they called "privacy homomorphisms". Their paper states, "although there are some truly inherent limitations on what can be accomplished, we shall see that it appears likely that there exist encryption functions which permit encrypted data to be operated on without preliminary decryption of the operands, for many sets of interesting operations. These special encryption functions we call 'privacy homomorphisms'; they form an interesting subset of arbitrary encryption schemes". Despite the optimism of Rivest, Adleman, and Dertouzos, fully homomorphic encryption remained out of reach for many years.

A number of cryptosystems are homomorphic with respect to one operation. For example, RSA and ElGamal encryption are homomorphic with respect to multiplication.

We recall that in (basic[1]) RSA, Alice's public key is (N, e) and private key is d, where N is a product of two large primes and where $de \equiv 1 \bmod \varphi(N)$. If $m \in \mathbb{Z}/N\mathbb{Z}$ is the plaintext, then the ciphertext is $c = m^e \bmod N$. To decrypt, Alice computes $c^d \bmod N = m$. If Bob encrypts messages m_1 and m_2 using Alice's public key (N, e), then the product of the resulting ciphertexts is the ciphertext of the product of the plaintexts m_1 and m_2, i.e., $(m_1^e \bmod N)(m_2^e \bmod N) = (m_1 m_2)^e \bmod N$. Thus, $\text{Decrypt}(c_1 \cdot c_2) = \text{Decrypt}(c_1) \cdot \text{Decrypt}(c_2)$, where $c_i = m_i^e \bmod N$ is the ciphertext corresponding to the plaintext m_i.

For ElGamal, suppose the private key is $x \in \{1, \ldots, n-1\}$ and the public key is $h = g^x \in G$, where G is a cyclic group of order n generated by g. If $m_1, m_2 \in G$ are plaintext messages, then the corresponding ciphertexts are of the form $c_i = (a_i, b_i) = (g^{r_i}, m_i h^{r_i}) \in G \times G$ for $i = 1$ and 2, where the r_i are chosen by the encryptor(s) at random in $\{1, \ldots, n-1\}$. Then

$$\begin{aligned}\text{Decrypt}(c_1 \cdot c_2) = \text{Decrypt}(a_1 a_2, b_1 b_2) &= ((a_1 a_2)^x)^{-1} b_1 b_2 \\ &= (a_1^x)^{-1} b_1 \cdot (a_2^x)^{-1} b_2 = \text{Decrypt}(c_1) \cdot \text{Decrypt}(c_2).\end{aligned}$$

There have been other encryption schemes with homomorphic properties. For example, the Goldwasser-Micali cryptosystem [**GM**] and its generalization the Paillier

[1]Note that "basic" RSA and ElGamal are not considered secure for most real world applications, and must be modified to be made secure.

cryptosystem [**Pa**] are homomorphic with respect to addition of plaintexts in the sense that

$$\text{Decrypt}(c_1 \cdot c_2) = m_1 + m_2,$$

but are not homomorphic with respect to multiplication of plaintexts.

In [**BonGN**], Boneh, Goh, and Nissim gave a partially homomorphic encryption scheme that can do one multiplication and any number of additions.

2.2. Gentry's FHE scheme and beyond. Craig Gentry solved the problem of how to do Fully Homomorphic Encryption in his Stanford PhD thesis [**G1, G2, G3**]. For the first time, there was now a scheme that could (inefficiently) do an arbitrary number of additions and multiplications.

Gentry's solution used ideal lattices, i.e., ideals in algebraic number fields. Given that one requires a homomorphic property with respect to two operations, it is natural that rings come into play. In [**G1**] and [**G2**], the rings Gentry used were of the form

$$R := \mathbb{Z}[x]/\langle x^N + 1\rangle \quad \text{and} \quad R_d := (\mathbb{Z}/d\mathbb{Z})[x]/\langle x^N + 1\rangle$$

where $N = 2^n$ (see §4 below). It was later realized that one can use the rings $\mathbb{Z}$ and $\mathbb{Z}/d\mathbb{Z}$ to construct schemes parallel to those that use the rings R and R_d (see §3 below). Brakerski's scheme in [**Br**] uses a tensor product operation on the ciphertexts rather than standard ring multiplication.

There have been a number of improvements, implementations, and new schemes. See for example [**SmV, DGHV, G4, SS, GH1, LaNV, GH2, BV2, BV1, CorMNT, LMSV, BrGV, GHS1, GHS2, CorNT**]. The NTRU encryption scheme [**HofPS**], which was developed in the late 1990's, turned out to be "somewhat homomorphic", and has been turned into an FHE scheme [**LTV**]. For some recent (at the time this article went to press) FHE schemes that are much more efficient than the original ones, see [**Br, BosLLN**].

2.3. Security. The primary known attacks on FHE schemes are variants of the LLL lattice basis reduction algorithm [**LLL**]. The security of almost all currently known schemes is based on the presumed difficulty of some lattice problem, such as finding an approximately shortest (non-zero) vector in a high dimensional lattice.

A number of FHE schemes use ideal lattices rather than arbitrary lattices. These are very special lattices, and it might turn out to be the case that lattice attacks are easier for ideal lattices than for generic lattices. This is an open question. At the moment, special attacks that work better for ideal lattices than for general lattices are not yet known.

Some of the recent FHE systems that are garnering a lot of interest are secure subject to the Ring-LWE (Learning With Errors) or decisional Ring-LWE Problem being difficult (see §5 below).

Using ideas from [**Br**], it is shown in [**BosLLN**] that the security of fully homomorphic variants of NTRU-based schemes can be based on the presumed difficulty of the Ring-LWE Problem.

2.4. Somewhat Homomorphic Encryption (SHE). Somewhat Homomorphic Encryption (SHE) schemes are encryption schemes that have some homomorphic properties but are not fully homomorphic. With Somewhat Homomorphic Encryption one can generally do a limited number of additions and multiplications, but each time one does an operation, it contributes "noise" to the ciphertext (see §3 for an example). Eventually the noise is so great that it is not possible to decrypt. Also, in SHE schemes the ciphertexts could get larger (message expansion), i.e., the compact ciphertexts requirement might be violated. In Gentry's initial work he started with an SHE scheme and then "bootstrapped" it to obtain an FHE scheme.

2.5. Bootstrapping. Gentry's original FHE papers and thesis introduced the idea of bootstrapping. One "bootstraps" to go from a (bootstrapable) somewhat homomorphic encryption scheme to a fully homomorphic encryption scheme.

To make an SHE scheme fully homomorphic, one can include as part of the public key an encryption of the private key. When a ciphertext gets too large or too noisy, the encryptor can then use the somewhat homomorphic encryption scheme to evaluate the decryption function applied to the ciphertext, using the encrypted private key. This re-encryption process produces a new encryption of the original plaintext, that is more compact and less noisy. For this to work, it is necessary for the somewhat homomorphic scheme to be "circular secure" (i.e., it must be able to securely encrypt its own private key) and capable of evaluating the function f = Decrypt and "a little more" (enough to allow homomorphic encryptions with respect to addition and multiplication; see the "augmented decryption circuits" in Definition 4 of [**G1**] or [**DGHV**]).

Gentry also uses what he calls "squashing" of the decryption circuit in order to simplify decryption enough so that it is among the functions that the somewhat homomorphic scheme can homomorphically evaluate correctly. Squashing converts an SHE scheme into a bootstrappable SHE scheme. In [**BV2**], Brakerski and Vaikuntanathan use "dimension-modulus reduction" to simplify the decryption circuit and avoid squashing. Another way to remove squashing is given in [**GH2**].

In [**BrGV**], Brakerski, Gentry, and Vaikuntanathan use "modulus switching" to reduce noise and lessen the need for bootstrapping. Modulus switching replaces a ciphertext mod p_1 with a ciphertext modulo a smaller modulus p_2 that decrypts to the same plaintext.

See [**G3**] for a nice analogy ("Alice's jewelry store", with jewelry fabricated in nested secure gloveboxes) that gives the idea of FHE and bootstrapping. See the survey article [**V1**] for a good description of modulus switching and other concepts from FHE.

2.6. Malleability. We remark that FHE schemes are always "malleable". In cryptography, malleability means that a ciphertext can be perturbed to create a new ciphertext that decrypts to a perturbation (in a known way) of the original plaintext. In a non-malleable encryption scheme, perturbing a ciphertext a little will generally

produce an invalid ciphertext, i.e., one that does not decrypt to a valid plaintext. Malleability is often an undesirable property in cryptography. For example, if an auction uses encrypted bids, and (an adversary) Mallory sees the encryption of Bob's bid, one wants it to be the case that Mallory cannot construct a new ciphertext that decrypts to a bid that is a dollar more than Bob's bid, i.e., one wants non-malleable encrypted bids.

There has been some work on obtaining partial or "targeted" non-malleability along with some limited homomorphic ability; see for example [**PR, BonSW, E**]. There are interesting open questions in this area.

3. Somewhat Homomorphic Encryption over the integers

We begin with a warm-up example from the introduction to [**DGHV**]. This example of a somewhat homomorphic encryption scheme comes in two flavors, symmetric key and public key. To keep it short, we will be very imprecise about parameter choices and other details.

We first give the symmetric key version. The shared key is an odd positive integer k. The message is a bit $m \in \{0, 1\}$. The encryptor chooses random integers q and r in a certain range, and so that $|2r| < k/2$, and computes the ciphertext

$$c = m + kq + 2r.$$

To decrypt, the decryptor computes ($c \bmod k$) $\bmod 2 = m$ where $a \bmod w$ means that one takes the representative of $a \bmod w$ in the range $(-w/2, w/2]$.

If $c_i = m_i + kq_i + 2r_i$ for $i = 1, 2$, then

$$c_1 + c_2 = (m_1 + m_2) + k(q_1 + q_2) + 2(r_1 + r_2),$$

$$c_1 \cdot c_2 = m_1 \cdot m_2 + k(m_1q_2 + m_2q_1 + kq_1q_2 + 2q_1r_2 + 2r_1q_2) + 2(m_1r_2 + r_1m_2 + 4r_1r_2).$$

Thus the noise grows, and after one does too many multiplications or additions, the decryption function no longer outputs the correct plaintext. The ciphertexts also blow up in size. This Somewhat Homomorphic Encryption scheme is not fully homomorphic, but in [**DGHV**] van Dijk et al. use Gentry's bootstrapping techniques to turn it into a Fully Homomorphic Encryption scheme.

A public key version, as in §3.1 of [**DGHV**], is as follows. The secret key is again an odd positive integer k. The public key now consists of the integers $x_i = kq_i + 2r_i$ for $i = 0, 1, \ldots, t$, where the q_i and r_i are as before, so each x_i can be viewed as an encryption of 0 under the symmetric key scheme. The x_i are taken so that x_0 is the largest, x_0 is odd, and $x_0 \bmod k$ is even, where again $x \bmod k$ is in the interval $(-k/2, k/2]$.

To encrypt a message bit $m \in \{0, 1\}$, the encryptor chooses a random subset S of $\{1, \ldots, t\}$ and a random integer r in a certain range. The ciphertext is

$$c = m + 2\sum_{i \in S} x_i + 2r \mod x_0.$$

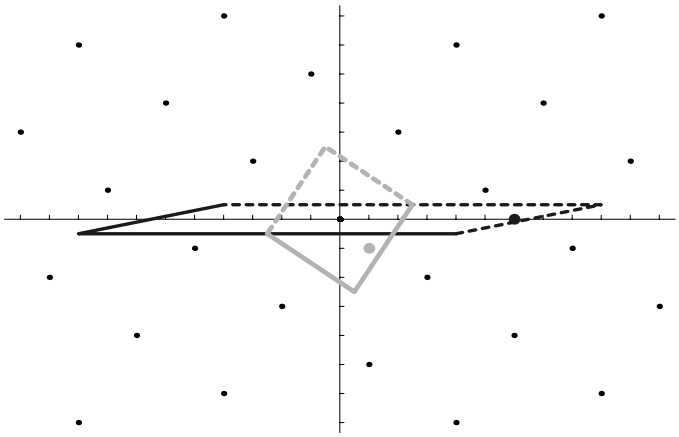
The decryptor computes ($c \bmod k$) $\bmod 2 = m$.

The security is based on the difficulty of the Approximate Common Divisor Problem, which is the problem of finding k, given a collection of integers of the form $\{kq_i + r_i\}_{i=0}^{t}$ with r_i "small". Approximate Common Divisor Problems were introduced in [**How**] and have been studied in [**CN, CoH**].

4. The Gentry, Smart-Vercauteren, and Gentry-Halevi SHE schemes

As an illustration of a lattice based system, we give a version of the Somewhat Homomorphic Encryption schemes that were introduced by Gentry in [**G1, G2**] and improved on by Smart and Vercauteren in [**SmV**] and by Gentry and Halevi in [**GH1**] (see also [**LMSV**]). In these schemes, the public key corresponds to a "bad" (skewed) basis for a lattice, while the private key is a "good" (more orthogonal) basis for the same lattice. The (N-dimensional) lattices are ideals in the ring of integers of the cyclotomic field of $2N$-th roots of unity. The plaintext is encoded as a (suitable) point in the ambient space $\mathbb{R}^N$. Encryption translates that point into the fundamental parallelepiped associated to the bad (public) basis. Decryption translates the ciphertext point into the fundamental parallelepiped associated to the good (private) basis. (See Figure 1 and the description near the end of §4.1.) The security relies partly on the fact that it is generally difficult to find a good, nearly orthogonal basis for a given lattice.

FIGURE 1. Encryption and Decryption



4.1. The scheme. We next give some of the details of a version of the scheme. Let

$$F(x) = x^N + 1 \in \mathbb{Z}[x]$$

with $N = 2^n$. Let θ be a root of $F(x)$; then θ is a primitive $2N$-th root of unity. Let

$$K = \mathbb{Q}[x]/\langle F(x)\rangle \cong \mathbb{Q}(\theta),$$

a CM-field of degree N over $\mathbb{Q}$. Let

$$v(x) = \sum_{i=0}^{N-1} v_i x^i \in \mathbb{Z}[x]$$

be a degree $N-1$ polynomial whose coefficients v_i are random t-bit integers for a suitably chosen t, and

$$V := \begin{pmatrix} v_0 & v_1 & \cdots & v_{N-1} \\ -v_{N-1} & v_0 & \cdots & v_{N-2} \\ & & \cdots & \\ -v_1 & -v_2 & \cdots & v_0 \end{pmatrix} \in \mathrm{M}_N(\mathbb{Z}).$$

The rows of V are the coefficients of $x^i v(x) \bmod F(x)$ for $i = 0, \ldots, N-1$. Let L denote the lattice in $\mathbb{Z}^N$ generated by the rows of V, let $\gamma = v(\theta) \in K$, let $\mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ denote the norm map, and let

$$d := \mathrm{N}_{K/\mathbb{Q}}(\gamma) = \det(V) = \det(L) = \text{resultant}(F, v).$$

Replace the random polynomial $v(x)$ if necessary, until you have found one for which d is odd and square-free. (In [**SmV**], they start with $v(x) \equiv 1 \bmod 2\mathbb{Z}[x]$ to ensure that d is odd, and they replace $v(x)$, if necessary, until they find one for which d is prime. In [**GH1**] they show that it is not necessary for d to be prime; it suffices to have d odd and square-free.)

Whenever A is a matrix whose rows $\{\mathbf{a}_1, \ldots, \mathbf{a}_N\}$ form a $\mathbb{Z}$-basis for a lattice $L \subset \mathbb{R}^N$, define

$$\mathcal{P}(A) := \{\sum_{i=1}^{N} \alpha_i \mathbf{a}_i : \alpha_i \in [-0.5, 0.5)\},$$

a (half-open) parallelepiped. This is the "fundamental parallelepiped" associated to A. Every element of $\mathbb{R}^N/L$ has a unique representative in $\mathcal{P}(A)$.

All reductions mod d will be taken in the range $[-d/2, d/2)$. Let $r \in [-d/2, d/2)$ denote the unique common root of $F(x)$ and $v(x)$ mod d. Let $r_i = r^i \pmod d$ and let

$$B := \begin{pmatrix} d & 0 & 0 & \cdots & 0 \\ -r_1 & 1 & 0 & \cdots & 0 \\ & \cdots & & & \\ -r_{N-1} & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathrm{M}_N(\mathbb{Z}).$$

Since d is odd and square-free, it follows that B is the Hermite Normal Form of the matrix V.

The public key now consists of d and r (or equivalently the matrix B), and the secret key is $v(x)$ (or the matrix V). To encrypt a bit $m \in \{0, 1\}$, choose a random noise polynomial $u(x) = \sum_{i=0}^{N-1} u_i x^i$ with each coefficient $u_i \in \{0, \pm 1\}$ taking values 1 and -1 with equal probability. Let $a(x) = m + 2u(x)$ and let

$$\mathbf{a} := (2u_0 + m, 2u_1, \ldots, 2u_{N-1})$$

be the vector of coefficients of $a(x)$. Let $\lceil \cdot \rfloor$ denote rounding to the nearest integer.

Let the ciphertext be

$$\mathbf{c} := \mathbf{a} - (\lceil \mathbf{a}B^{-1} \rfloor B) = (m + 2u(r) \mod d, 0, \ldots, 0),$$

which is the translation of $\mathbf{a}$ to the parallelepiped $\mathcal{P}(B)$ (where translation means that one subtracts lattice vectors until one lands in the fundamental parallelepiped).

To decrypt a ciphertext $\mathbf{c}$, let

$$\mathbf{a}_1 := \mathbf{c} - (\lceil \mathbf{c}V^{-1} \rfloor V) = (a_0, \ldots, a_{N-1}),$$

which is the translation of $\mathbf{c}$ to the parallelepiped $\mathcal{P}(V)$, and compute $m = a_0 \pmod 2$. As shown on p. 145 of [**GH1**], decryption works (i.e., $\mathbf{a}_1 = \mathbf{a}$) as long as the absolute value of every entry in $\mathbf{a}V^{-1}$ is less than $\frac{1}{2}$.

In Figure 1, the small dots are the lattice. The light gray point represents the plaintext, the (inside of the) light gray diamond represents the fundamental parallelepiped $\mathcal{P}(V)$, the (inside of the) dark parallelogram represents the fundamental parallelepiped $\mathcal{P}(B)$, and the large dark point, which is the ciphertext, is the translation to $\mathcal{P}(B)$ of the light gray point.

The rows of the matrix B are a "bad", i.e., skewed basis for the lattice L, while the rows of V are a "good" (secret) basis for L. If the rows of V are sufficiently orthogonal, and if the plaintext point is chosen in a suitable way, then decryption yields the original plaintext point.

The scheme is homomorphic because its multiplication and addition are just multiplication and addition in the ring of integers of the cyclotomic field K.

4.2. Security. The security of the above scheme is based on the simultaneous difficulty of the following problems. (Note that more recent FHE schemes do not rely on SPIP, PCP, or SSSP, so interest in these problems might be more theoretical or mathematical than practical.)

The **Small Principal Ideal Problem (SPIP)** is the problem, given a principal ideal in either Hermite Normal Form (i.e., the matrix B) or two element representation (i.e., $\langle d, \theta - r \rangle$), of finding a "small" generator (e.g., $v(\theta)$) for it. If the SPIP is sufficiently hard, that would thwart a key recovery attack, wherein an adversary who knows the public key (B or (d, r)) tries to find the secret key ($v(x)$).

Security against an attack where the adversary tries to find the plaintext, given a ciphertext, is closely related to the difficulty of the **Closest Vector Problem (CVP)** for ideal lattices. This is the problem of finding a closest lattice point to a given point in the ambient space.

Another type of security is "semantic security". The requirement for semantic security is that an adversary, who is presented with a ciphertext that is either an encryption of 0 or an encryption of 1, cannot distinguish which it is with probability greater than $\frac{1}{2} + \epsilon$ of getting the correct answer. The semantic security of the scheme is related to a new problem, that Smart and Vercauteren call the **Polynomial Coset Problem (PCP)**. The Polynomial Coset Problem is the problem of distinguishing

between a random element of $\mathbb{Z}/d\mathbb{Z}$ and an element of the form $f(r) \bmod d$, where $f(x) \in \mathbb{Z}[x]$ is random (and unknown) with small coefficients and r is the common root of $F(x)$ and $v(x) \bmod d$. The paper [**SmV**] states that the Polynomial Coset Problem is akin to Gentry's Ideal Coset Problem from [**G1**]. These problems can be viewed as versions of the Bounded Distance Decoding problem from coding theory.

Gentry, Smart-Vercauteren and Gentry-Halevi "bootstrap" their somewhat homomorphic encryption schemes into fully homomorphic encryption schemes using a re-encryption algorithm. Making this cryptographically secure requires an additional security assumption, namely the difficulty of a decisional version of the **Sparse Subset-Sum Problem (SSSP)**, i.e., it should be difficult to distinguish between random subsets of $\mathbb{Z}/d\mathbb{Z}$ and those that have sparse subsets that sum to 0. Here, bootstrapping augments the public key with a "hint" about the secret key, namely, with a large set of vectors that has a very sparse subset that sums to the secret key.

4.3. Why F and v have exactly one common root mod d. Since it is not in the FHE literature, we give a proof that $F(x)$ and $v(x)$ have a unique common root mod d. This shows the use of some algebraic number theory in FHE. The next result allows for a more general polynomial $F(x)$. As usual, $\mathcal{O}_K$ denotes the ring of integers in the number field K.

LEMMA 1. *Suppose $F(x), v(x) \in \mathbb{Z}[x]$. Suppose that $F(x)$ is monic and irreducible, and $\theta \in \bar{\mathbb{Q}}$ is a root of F. Let $K = \mathbb{Q}[x]/\langle F(x)\rangle \cong \mathbb{Q}(\theta)$ and suppose $K/\mathbb{Q}$ is a Galois extension. Let $\gamma = v(\theta)$ and suppose that $\mathrm{N}_{K/\mathbb{Q}}(\gamma)$ is square-free and relatively prime to the discriminant of K. Then $F(x) \bmod \langle\gamma\rangle$ and $v(x) \bmod \langle\gamma\rangle$ have exactly one common root in $\mathcal{O}_K/\langle\gamma\rangle$, namely $\theta \bmod \langle\gamma\rangle$.*

PROOF. Since $v(\theta) = \gamma$ and $F(\theta) = 0$ both map to 0 under the projection map $\mathcal{O}_K \to \mathcal{O}_K/\langle\gamma\rangle$, it follows that θ is a common root of $F(x) \bmod \langle\gamma\rangle$ and $v(x) \bmod \langle\gamma\rangle$. Since $K/\mathbb{Q}$ is Galois, $F(x)$ splits completely in $K[x]$, so the reductions mod $\langle\gamma\rangle$ of the roots of $F(x)$ are the roots of $F(x) \bmod \langle\gamma\rangle$. Thus any other common root is the reduction mod $\langle\gamma\rangle$ of a root of $F(x)$, so it is $\sigma(\theta)$ for some non-identity $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. But $v(\sigma(\theta)) = \sigma(v(\theta)) = \sigma(\gamma)$, which cannot be 0 mod $\langle\gamma\rangle$, since $\gcd(\sigma(\gamma), \gamma) = 1$, as follows.

Factor $\gamma\mathcal{O}_K = \prod_i \mathfrak{p}_i$ with prime ideals $\mathfrak{p}_i$ of $\mathcal{O}_K$. Since $\mathrm{N}_{K/\mathbb{Q}}(\gamma)$ is square-free and relatively prime to the discriminant of K, it follows that:

(a) each $\mathfrak{p}_i$ has degree one (i.e., its norm is a prime in $\mathbb{Z}$),
(b) the different $\mathfrak{p}_i$'s have distinct residue characteristics, and
(c) $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$ for all i and j.

To obtain (c), note that if $\sigma(\mathfrak{p}_i) = \mathfrak{p}_i$, then σ would be in the decomposition group for $\mathfrak{p}_i$, whose order is the degree of $\mathfrak{p}_i$, which is 1 by (a). Part (c) now follows from (b). Since $\sigma(\gamma)\mathcal{O}_K = \prod_i \sigma(\mathfrak{p}_i)$, it now follows that $\gcd(\sigma(\gamma), \gamma) = 1$. □

5. LWE and Ring-LWE

A promising recent development is to create Fully Homomorphic Encryption schemes whose security is based on the difficulty of the LWE Problem (introduced in [**R**]) or the Ring-LWE Problem (introduced in [**LyPR**]). These FHE schemes are more efficient than earlier schemes, with short ciphertexts.

LWE stands for Learning With Errors. A version of the LWE Problem is as follows. If F is a field and $v = (v_1, \ldots, v_n), w = (w_1, \ldots, w_n) \in F^n$, let $\langle v, w \rangle$ denote the usual inner product $\sum_{j=1}^{n} v_j w_j$. Take p prime, of size polynomial in a parameter n. For uniformly random $a_i \in \mathbb{F}_p^n$, and "noise" $e_i \in \mathbb{Z}$ chosen via a probability distribution (usually Gaussian) that outputs e_i with $|e_i|$ much smaller than p, given polynomially (in n) many pairs $(a_i, b_i = \langle a_i, s \rangle + e_i \mod p)$, find $s \in \mathbb{F}_p^n$. Here, the e_i's are the errors, and the problem is to learn the secret s, even in the presence of errors. If there are no errors, i.e., all $e_i = 0$, then one can easily recover s using linear algebra, given enough pairs (a_i, b_i). When $p = 2$ the Learning With Errors Problem is known as the Learning Parity with Noise Problem.

In the decisional version one needs to distinguish such ordered pairs (a_i, b_i) from uniformly random pairs $(a_i, u_i) \in \mathbb{F}_p^n \times \mathbb{F}_p$. By [**R, Pe**], this problem is at least as hard as (variants of) the problem of finding short vectors in lattices.

Next, following [**BV2**], we give a simplification of a symmetric key somewhat homomorphic encryption scheme whose security is based on the decisional version of LWE. The secret key is a random $s \in \mathbb{F}_p^n$. To encrypt a plaintext bit $m \in \{0, 1\}$, choose a random $a \in \mathbb{F}_p^n$ and a "noise" e. Compute $b := \langle a, s \rangle + 2e + m \in \mathbb{F}_p$. The ciphertext is $(a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p$. To decrypt, compute $b - \langle a, s \rangle \equiv 2e + m \pmod p$ and reduce mod p to get $2e + m$ (since $|e| \ll p$). Now reduce mod 2 to obtain m. The scheme is homomorphic with respect to addition, until too much noise accumulates, and it is shown in [**GHV**] that a variant of the scheme can do one homomorphic multiplication but with a large ciphertext expansion. In [**BV2**] it is shown how to turn this into a fully homomorphic encryption scheme (without the need for squashing).

In Ring-LWE, R is a ring. The Ring-LWE Problem is to find s, given polynomially many $(a_i, b_i) \in R \times R$ with $b_i = a_i s + e_i$ where the a_i's are uniformly random in R, s is random in R, and the e_i's are "small" in R.

In the decisional version of Ring-LWE, one needs to distinguish such ordered pairs (a_i, b_i) from uniformly random $(a_i, u_i) \in R \times R$.

Next, taken from [**BV1**], is a simplified symmetric key somewhat homomorphic encryption scheme whose security is based on the decisional version of Ring-LWE. Fix an odd prime p and let R_p denote the ring $\mathbb{F}_p[x]/\langle x^N + 1 \rangle$ where $N = 2^n$. The secret key is a random $s \in R_p$. To encrypt $m \in \mathbb{F}_2[x]/\langle x^N + 1 \rangle$, lift m to a polynomial in $\mathbb{Z}[x]$ of degree $< N$ with coefficients in $\{0, 1\}$ and (reduce mod p and mod $x^N + 1$ to) view it as an element $\hat{m}$ of R_p. Then choose a random $a \in R_p$ and a "noise" e, and compute $b := as + 2e + \hat{m} \in R_p$. The ciphertext is $(a, b) \in R_p \times R_p$. To decrypt, compute $b - as \pmod 2 = m$. Security follows from decisional Ring-LWE for R_p, since under the assumption that decisional Ring-LWE is a hard problem, and using

the fact that p is odd, pairs $(a, as + 2e)$ are indistinguishable from pairs (a, u) where u is uniformly random in R_p. Again, this can be turned into a fully homomorphic encryption scheme (see [**BV1**]).

Fully homomorphic encryption schemes based on Ring-LWE are more efficient than those based on standard LWE. However, Ring-LWE uses lattices coming from ideals in algebraic number fields. As mentioned earlier, it is not known whether cryptosystems based on ideal lattices are more vulnerable to attack than those based on general lattices.

References

[BonGN] D. Boneh, E-J. Goh, and K. Nissim, *Evaluating 2-DNF formulas on ciphertexts*, in Theory of Cryptography—TCC'05, Lect. Notes in Comp. Sci. **3378** (2005), Springer, 325-341.

[BonSW] D. Boneh, G. Segev, and B. Waters, *Targeted malleability: homomorphic encryption for restricted computations*, in Innovations in Theoretical Computer Science 2012 (ITCS 2012), ACM (2012), 350–366.

[BosLLN] J. W. Bos, K. Lauter, J. Loftus, M, Naehrig, *Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme*, Cryptology ePrint Archive: Report 2013/075, `http://eprint.iacr.org/2013/075`.

[Br] Z. Brakerski, *Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP*, in Advances in Cryptology—CRYPTO 2012, Lect. Notes in Comp. Sci. **7417** (2012), Springer, 868–886.

[BrGV] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, *(Leveled) fully homomorphic encryption without bootstrapping*, in Innovations in Theoretical Computer Science (ITCS) 2012, ACM, 309–325.

[BV1] Z. Brakerski and V. Vaikuntanathan, *Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages*, in Advances in Cryptology—CRYPTO 2011, Lect. Notes in Comp. Sci. **6841** (2011), Springer, 505–524.

[BV2] Z. Brakerski and V. Vaikuntanathan, *Efficient Fully Homomorphic Encryption from (Standard) LWE*, in Proceedings of 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS 2011), IEEE, 97–106.

[CN] Y. Chen and P. Q. Nguyen, *Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers*, in Advances in Cryptology—EUROCRYPT 2012, Lect. Notes in Comp. Sci. **7237** (2012), Springer, 502–519.

[CoH] H. Cohn and N. Heninger, *Approximate common divisors via lattices*, to appear in Algorithmic Number Theory (ANTS X), Mathematical Sciences Publishers; `http://arxiv.org/abs/1108.2714`.

[CorMNT] J-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, *Fully homomorphic encryption over the integers with shorter public keys*, in Advances in Cryptology—CRYPTO 2011, Lect. Notes in Comp. Sci. **6841** (2011), Springer, 487-504.

[CorNT] J-S. Coron, D. Naccache, and M. Tibouchi, *Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers*, in Advances in Cryptology—EUROCRYPT 2012, Lect. Notes in Comp. Sci. **7237** (2012), Springer, 446–464.

[DGHV] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, *Fully Homomorphic Encryption over the Integers*, in Advances in Cryptology—EUROCRYPT 2010, Lect. Notes in Comp. Sci. **6110** (2010), Springer, 24–43.

[E] K. Emura, G. Hanaoka, G. Ohtake, T. Matsuda, S. Yamada, *Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption*, in Public-Key Cryptography—PKC 2013, Lect. Notes in Comp. Sci. **7778** (2013), Springer, 32–50.

[G1] C. Gentry, *Fully homomorphic encryption using ideal lattices*, in Proceedings of the 41st ACM Symposium on Theory of Computing—STOC 2009, ACM, New York (2009), 169–178.

[G2] C. Gentry, *A fully homomorphic encryption scheme*, Stanford University PhD thesis, 2009, `http://crypto.stanford.edu/craig/craig-thesis.pdf`.

[G3] C. Gentry, *Computing arbitrary functions of encrypted data*, Communications of the ACM **53** (2010), 97–105.

[G4] C. Gentry, *Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness*, in Advances in Cryptology—CRYPTO 2010, Lect. Notes in Comp. Sci. **6223** (2010), Springer, 116–137.

[GH1] C. Gentry and S. Halevi, *Implementing Gentry's Fully-Homomorphic Encryption Scheme*, in Advances in Cryptology—EUROCRYPT 2011, Lect. Notes in Comp. Sci. **6632**, (2011), Springer, 129–148.

[GH2] C. Gentry and S. Halevi, *Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits*, `http://eprint.iacr.org/2011/279`.

[GHS1] C. Gentry, S. Halevi, and N. P. Smart, *Better Bootstrapping in Fully Homomorphic Encryption*, Public Key Cryptography 2012, 1–16.

[GHS2] C. Gentry, S. Halevi, and N. P. Smart, *Fully Homomorphic Encryption with Polylog Overhead*, in Advances in Cryptology—EUROCRYPT 2012, Lect. Notes in Comp. Sci. **7237** (2012), Springer, 465–482.

[GHV] C. Gentry, S. Halevi, and V. Vaikuntanathan, *A Simple BGN-Type Cryptosystem from LWE*, in Advances in Cryptology—EUROCRYPT 2010, Lect. Notes in Comp. Sci. **6110** (2010), Springer, 506–522.

[GM] S. Goldwasser and S. Micali, *Probabilistic encryption and how to play mental poker keeping secret all partial information*, in Proceedings of the 14th ACM Symposium on Theory of Computing—STOC 1982, ACM (1982), 365-377.

[H] B. Hayes, *Alice and Bob in Cipherspace*, American Scientist **100** (2012), 362–367.

[HofPS] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, in Proceedings of ANTS-III—Algorithmic Number Theory Third International Symposium, Lect. Notes in Comp. Sci. **1423**, (1998), Springer, 267–288.

[How] N. Howgrave-Graham, *Approximate integer common divisors*, in Cryptography and Lattices, International Conference, CaLC 2001, Lect. Notes in Comp. Sci. **2146** (2001), Springer, 51-66.

[LaNV] K. Lauter, M. Naehrig, and V. Vaikuntanathan, *Can homomorphic encryption be practical?*, in Proceedings of the 3rd ACM Cloud Computing Security Workshop, CCSW 2011, ACM, New York, 113–124.

[LLL] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515-534.

[LMSV] J. Loftus, A. May, N. P. Smart, F. Vercauteren, *On CCA-Secure Somewhat Homomorphic Encryption*, in Selected Areas in Cryptography 2011, Lect. Notes in Comp. Sci. **7118** (2012), Springer, 55–72.

[LTV] A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan, *On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption*, in Proceedings of the 44th symposium on Theory of Computing—STOC 2012, ACM, New York (2012), 1219–1234.

[LyPR] V. Lyubashevsky, C. Peikert, and O. Regev, *On Ideal Lattices and Learning with Errors over Rings*, in Advances in Cryptology—EUROCRYPT 2010, Lect. Notes in Comp. Sci. **6110** (2010), Springer, 1–23.

[Pa] P. Paillier, *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*, in Advances in Cryptology—EUROCRYPT '99, Lect. Notes in Comp. Sci. **1592** (1999), Springer, 223–238.

[Pe] C. Peikert, *Public-key cryptosystems from the worst-case shortest vector problem*, in Proceedings of the 41st ACM Symposium on Theory of Computing—STOC 2009, ACM, New York (2009), 333-342.

[PR] M. Prabhakaran and M. Rosulek, *Homomorphic Encryption with CCA Security*, in Proceedings of Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Part II, Lect. Notes in Comp. Sci. **5126** (2008), Springer, 667–678.

[R] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, in Proceedings of the 37th Annual ACM Symposium on Theory of Computing—STOC 2005, ACM, New York (2005), 84-93; full version in J. ACM **56** (2009).

[RAD] R. Rivest, L. Adleman, and M. Dertouzos, *On Data Banks and Privacy Homomorphisms*, in Foundations of Secure Computation, Academic Press, New York (1978), 169–180.

[SmV] N. P. Smart and F. Vercauteren, *Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes*, in Public Key Cryptography—PKC 2010, Lect. Notes in Comp. Sci. **6056** (2010), Springer, 420–443.

[SS] D. Stehlé and R. Steinfeld, *Faster fully homomorphic encryption*, in Advances in Cryptology—ASIACRYPT 2010, Lect. Notes in Comp. Sci. **6477** (2010), Springer, 377-394.

[V1] V. Vaikuntanathan, *Computing Blindfolded: New Developments in Fully Homomorphic Encryption*, in Proceedings of 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS 2011), IEEE, 5–16.

[V2] V. Vaikuntanathan, *How to Compute on Encrypted Data*, in INDOCRYPT 2012, Lect. Notes in Comp. Sci. **7668** (2012), Springer, 1–15.

Department of Mathematics, University of California, Irvine, CA 92697
E-mail address: asilverb@math.uci.edu

Revisiting the Gentry-Szydlo Algorithm

H. W. Lenstra[1] and A. Silverberg[2⋆]

[1] Mathematisch Instituut
Universiteit Leiden
The Netherlands
hwl@math.leidenuniv.nl

[2] Department of Mathematics
University of California, Irvine
Irvine, CA, USA
asilverb@uci.edu

Abstract. We put the Gentry-Szydlo algorithm into a mathematical framework, and show that it is part of a general theory of "lattices with symmetry". For large ranks, there is no good algorithm that decides whether a given lattice has an orthonormal basis. But when the lattice is given with enough symmetry, we can construct a provably deterministic polynomial time algorithm to accomplish this, based on the work of Gentry and Szydlo. The techniques involve algorithmic algebraic number theory, analytic number theory, commutative algebra, and lattice basis reduction. This sheds new light on the Gentry-Szydlo algorithm, and the ideas should be applicable to a range of questions in cryptography.

Keywords: lattices, Gentry-Szydlo algorithm, ideal lattices, lattice-based cryptography

1 Introduction

In §7 of [6], Gentry and Szydlo introduced some powerful new ideas that combined in a clever way lattice basis reduction and number theory. They used these ideas to cryptanalyze NTRU Signatures. The recent interest in Fully Homomorphic Encryption (FHE) and in the candidate multilinear maps of Garg-Gentry-Halevi [2] bring the Gentry-Szydlo results once again to the fore. Gentry's first FHE scheme [3] used ideal lattices, as have a number of subsequent schemes. Fully Homomorphic Encryption is performed more efficiently with ideal lattices than with general lattices. However, ideal lattices are special, with much structure ("symmetries") that has the potential to be exploited. In his thesis [4], Gentry mentions that the Gentry-Szydlo attack on NTRU signatures can be used to attack principal ideal lattices in the ring $\mathbb{Z}[X]/(X^n - 1)$, if the lattice has an orthonormal basis.

⋆ This material is based on research sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750-13-2-0054. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

As Gentry pointed out [5], the Gentry-Szydlo algorithm "seems to be a rather crazy, unusual combination of LLL with more 'algebraic' techniques. It seems like it should have more applications—e.g., perhaps to breaking or weakening ideal lattices." Generalizing or improving the Gentry-Szydlo algorithm would potentially affect the security of all cryptography that is built from ideal lattices, or whose security is based on hard problems for ideal lattices. Candidate multilinear maps were recently cryptanalyzed using the Gentry-Szydlo algorithm. As remarked by Garg, Gentry, and Halevi in [2], their "new algebraic/lattice attacks are extensions of an algorithm by Gentry and Szydlo, which combines lattice reduction and Fermat's Little Theorem in a clever way to solve a relative norm equation in a cyclotomic field."

The Gentry-Szydlo algorithm has been viewed by some as magic [11]. In this paper we revisit the algorithm and put it in a mathematical framework, in order to make it easier to understand, generalize, and improve on. That should help make it more widely applicable in cryptographic applications. We embed the algorithm in a wider theory that we refer to as "lattices with symmetry".

The algorithm of Gentry and Szydlo can be viewed as a way to find an orthonormal basis (if one exists) for an ideal lattice. Determining whether a lattice has an orthonormal basis is a difficult algorithmic problem that is easier when the lattice has many symmetries. In this paper we solve this problem when the lattice comes with a sufficiently large abelian group of automorphisms, and we show how the Gentry-Szydlo algorithm is a special case of this result.

Our algorithm runs in deterministic polynomial time, whereas [6] relies on a probabilistic algorithm. Also, our setting is more general (our theory applies to arbitrary finite abelian groups, where [6] considers only cyclic groups of odd prime order), thereby covering other cases of potential cryptographic interest.

Briefly, our main result is as follows (see §2 for background information). If G is a finite abelian group and $u \in G$ has order 2, define a G-lattice to be a lattice L with a group homomorphism $G \to \mathrm{Aut}(L)$ that takes u to -1. The "standard" G-lattice is the modified group ring $\mathbb{Z}\langle G\rangle = \mathbb{Z}[G]/(u+1)$. A G-isomorphism is an isomorphism of lattices that respects the G-actions.

Theorem 1.1 *There is a deterministic polynomial time algorithm that, given a finite abelian group G, an element $u \in G$ of order 2, and a G-lattice L, decides whether L and $\mathbb{Z}\langle G\rangle$ are G-isomorphic, and if they are, exhibits a G-isomorphism.*

The ingredients include the technique invented by Gentry and Szydlo in [6], lattice basis reduction, commutative algebra (finite rings and tensor algebras), analytic number theory, and algorithmic algebraic number theory. The graded tensor algebra Λ introduced in §3.4 is in a sense the hero of our story. It replaces Gentry's and Szydlo's polynomial chains. In §7 of [6], taking powers of an ideal in the ring $R = \mathbb{Z}[X]/(X^n - 1)$ required complicated bookkeeping, via polynomial chains and lattice basis reduction to avoid coefficient blow-up. We do away with this, by using the

module structure of the ideal, rather than its ideal structure. More precisely, an ideal in a commutative ring R is the same as an R-module M along with an embedding $M \hookrightarrow R$ of R-modules. While Gentry and Szydlo use the embedding, we observe that one can avoid coefficient blow-up by using the module structure of M but not the actual embedding. We replace ideal multiplication with tensor products of lattices.

In §2 we introduce the concept of a G-lattice, and in §2.3 we show that Theorem 1.1 implies the result of Gentry and Szydlo. In §3–§4 we introduce invertible G-lattices, of which the ideal lattices considered by Gentry and Szydlo are examples, and give the concepts and results that we use to state our new algorithm and prove its correctness. We explicitly present the algorithm in §5.

2 G-lattices and the modified group ring

In this section we explain some notation and concepts that we use in our main result.

2.1 Lattices and G-lattices

We first give some background on lattices (see also [10]), and introduce G-lattices.

Definition 2.1 *A* **lattice** *or* **integral lattice** *is a finitely generated abelian group L with a map $\langle \cdot, \cdot \rangle : L \times L \to \mathbb{Z}$ that is*

- *bilinear: $\langle x, y+z \rangle = \langle x, y \rangle + \langle x, z \rangle$ and $\langle x+y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ for all $x, y, z \in L$,*
- *symmetric: $\langle x, y \rangle = \langle y, x \rangle$ for all $x, y \in L$, and*
- *positive definite: $\langle x, x \rangle > 0$ if $0 \neq x \in L$.*

As a group, L is isomorphic to $\mathbb{Z}^n$ for some n, which is called the **rank** of L. In algorithms, a lattice is specified by a Gram matrix $(\langle b_i, b_j \rangle)_{i,j=1}^n$ associated to a $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$.

Definition 2.2 *The* **standard lattice** *of rank n is $L = \mathbb{Z}^n$ with $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$. Its Gram matrix is the $n \times n$ identity matrix I_n.*

Definition 2.3 *A lattice L is* **unimodular** *if the map $L \to \mathrm{Hom}(L, \mathbb{Z})$ that takes each $x \in L$ to the map $y \mapsto \langle x, y \rangle$ is bijective. Equivalently, L is unimodular if its Gram matrix has determinant 1.*

Definition 2.4 *An* **isomorphism** *$L \xrightarrow{\sim} M$ of lattices is a group isomorphism $\varphi : L \xrightarrow{\sim} M$ that respects the lattice structures, i.e., $\langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$ for all $x, y \in L$. If such a map φ exists, then L and M are* **isomorphic** *lattices. An* **automorphism** *of a lattice L is an isomorphism from L onto itself. The set of automorphisms of L is a finite group $\mathrm{Aut}(L)$ whose center contains -1 (represented by $-I_n$).*

In algorithms, isomorphisms are specified by their matrices on the given bases of L and M.

Examples 2.5 (i) *"Random" lattices have* $\mathrm{Aut}(L) = \{\pm 1\}$.
(ii) *Letting* S_n *denote the symmetric group on* n *letters and* $\rtimes$ *denote semidirect product, then* $\mathrm{Aut}(\mathbb{Z}^n) \cong \{\pm 1\}^n \rtimes S_n$. *(The standard basis vectors can be permuted, and negatives taken.)*
(iii) *If* L *is the equilateral triangular lattice in the plane, then* $\mathrm{Aut}(L)$ *is the symmetry group of the regular hexagon, which is a dihedral group of order* 12.

From now on, suppose that G is a finite abelian group, and $u \in G$ is a fixed element of order 2.

Definition 2.6 *A* G**-lattice** *is a lattice* L *together with a group homomorphism* $f : G \to \mathrm{Aut}(L)$ *such that* $f(u) = -1$. *For each* $\sigma \in G$ *and* $x \in L$, *define* $\sigma x \in L$ *by* $\sigma x = f(\sigma)(x)$.

The abelian group G is specified by a multiplication table. The G-lattice L is specified as a lattice along with, for each $\sigma \in G$, the matrix describing the action of σ on L.

Definition 2.7 *If* L *and* M *are* G*-lattices, then a* G**-isomorphism** *is an isomorphism* $\varphi : L \xrightarrow{\sim} M$ *of lattices that respects the* G*-actions, i.e.,* $\varphi(\sigma x) = \sigma\varphi(x)$ *for all* $x \in L$ *and* $\sigma \in G$. *If such an isomorphism exists, we say that* L *and* M *are* G*-isomorphic, or isomorphic as* G*-lattices.*

2.2 The Modified Group Ring $\mathbb{Z}\langle G\rangle$

We define a modified group ring $A\langle G\rangle$ whenever A is a commutative ring. We will usually take $A = \mathbb{Z}$, but will also take $A = \mathbb{Z}/m\mathbb{Z}$. We consider $A\langle G\rangle$ rather than the standard group ring $A[G]$, since G-lattices become $\mathbb{Z}\langle G\rangle$-modules. Also, it allows us to include the cyclotomic rings $\mathbb{Z}[X]/(X^{2^k}+1)$ in our theory.

The group ring $A[G]$ is the set of formal sums $\sum_{\sigma\in G} a_\sigma\sigma$ with $a_\sigma \in A$, with addition defined by

$$\sum_{\sigma\in G} a_\sigma\sigma + \sum_{\sigma\in G} b_\sigma\sigma = \sum_{\sigma\in G}(a_\sigma + b_\sigma)\sigma$$

and multiplication defined by

$$(\sum_{\sigma\in G} a_\sigma\sigma)(\sum_{\tau\in G} b_\tau\tau) = \sum_{\rho\in G}(\sum_{\sigma\tau=\rho} a_\sigma b_\tau)\rho.$$

For example, if G is a cyclic group of order m and g is a generator, then as rings $\mathbb{Z}[X]/(X^m-1) \cong \mathbb{Z}[G]$ via the map $\sum_{i=0}^{m-1} a_i X^i \mapsto \sum_{i=0}^{m-1} a_i g^i$.

Definition 2.8 *If A is a commutative ring, then writing 1 for the identity element of the group G, we define the* **modified group ring**

$$A\langle G\rangle = A[G]/(u+1).$$

Every G-lattice is a $\mathbb{Z}\langle G\rangle$-module, where one uses the G-action on L to define ax whenever $x \in L$ and $a \in \mathbb{Z}\langle G\rangle$.

Definition 2.9 *Define the* **scaled trace function** $t : A\langle G\rangle \to A$ *by*

$$t(\sum_{\sigma\in G} a_\sigma \sigma) = a_1 - a_u.$$

Then t is the (additive) group homomorphism satisfying $t(1) = 1$, $t(u) = -1$, and $t(\sigma) = 0$ if $\sigma \in G$ and $\sigma \neq 1, u$.

Definition 2.10 *For $a = \sum_{\sigma\in G} a_\sigma\sigma \in A\langle G\rangle$, define $\overline{a} = \sum_{\sigma\in G} a_\sigma\sigma^{-1}$.*

The map $a \mapsto \overline{a}$ is a ring automorphism of $A\langle G\rangle$. Since $\overline{\overline{a}} = a$, it is an involution. (An involution is a map that is its own inverse.) In practice, this map plays the role of complex conjugation.

Remark 2.11 *If L is a G-lattice and $x, y \in L$, then $\langle \sigma x, \sigma y\rangle = \langle x, y\rangle$ for all $\sigma \in G$. It follows that $\langle ax, y\rangle = \langle x, \overline{a}y\rangle$ for all $a \in \mathbb{Z}\langle G\rangle$.*

Definition 2.12 *For $x, y \in \mathbb{Z}\langle G\rangle$ define $\langle x, y\rangle_{\mathbb{Z}\langle G\rangle} = t(x\overline{y})$.*

Let $n = |G|/2 \in \mathbb{Z}$.

Definition 2.13 *Let S be a set of coset representatives of $G/\langle u\rangle$ (i.e., $\#S = n$ and $G = S \sqcup uS$), and for simplicity take S so that $1 \in S$.*

The following result is straightforward.

Proposition 2.14 (i) *The additive group of the ring $\mathbb{Z}\langle G\rangle$ is a G-lattice of rank n, with lattice structure defined by $\langle x, y\rangle_{\mathbb{Z}\langle G\rangle}$ and G-action defined by $\sigma x = \sigma x$ where the right-hand side is ring multiplication in $\mathbb{Z}\langle G\rangle$.*

(ii) *As lattices, $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}^n$.*

(iii) $\mathbb{Z}\langle G\rangle = \{\sum_{\sigma\in S} a_\sigma\sigma : a_\sigma \in \mathbb{Z}\} = \bigoplus_{\sigma\in S} \mathbb{Z}\sigma$ *and* $t(\sum_{\sigma\in S} a_\sigma\sigma) = a_1$.

Definition 2.15 *We call $\mathbb{Z}\langle G\rangle$ the* **standard G-lattice**.

Example 2.16 *Suppose $G = H \times \langle u\rangle$ with $H \cong \mathbb{Z}/n\mathbb{Z}$. Then $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[H] \cong \mathbb{Z}[X]/(X^n - 1)$ as rings and as lattices. When n is odd (so G is cyclic), then (by sending X to $-X$) we have $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[X]/(X^n - 1) \cong \mathbb{Z}[X]/(X^n + 1)$.*

Remark 2.17 *The ring $\mathbb{Z}\langle G\rangle$ is an integral domain (i.e., no zero divisors) if and only if G is cyclic and n is a power of 2. If G is cyclic of order 2^r, then $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[\zeta_{2^r}]$.*

2.3 Ideal Lattices

Example 2.18 *Suppose I is an ideal in the ring $\mathbb{Z}\langle G\rangle$ and $w \in \mathbb{Z}\langle G\rangle$. Suppose that $I\overline{I} = \mathbb{Z}\langle G\rangle \cdot w$ and $\psi(w) \in \mathbb{R}_{>0}$ for all ring homomorphisms $\psi : \mathbb{Z}\langle G\rangle \to \mathbb{C}$. It follows that the ideal I has finite index in $\mathbb{Z}\langle G\rangle$, that $\overline{w} = w$, and that w is not a zero divisor. Define the G-lattice $L_{(I,w)}$ to be I with G-action given by multiplication in $\mathbb{Z}\langle G\rangle$, and with lattice structure defined by*

$$\langle x, y\rangle_{I,w} = t\left(\frac{x\overline{y}}{w}\right)$$

with t as in Definition 2.9. (Note that $\frac{x\overline{y}}{w} \in \mathbb{Z}\langle G\rangle$ since w generates the ideal $I\overline{I}$.) In particular, $L_{(\mathbb{Z}\langle G\rangle,1)} = \mathbb{Z}\langle G\rangle$.

The lattice $L_{(I,w)}$ is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if there exists $v \in \mathbb{Z}\langle G\rangle$ such that $I = (v)$ and $w = v\overline{v}$. Further, knowing *such a G-isomorphism is equivalent to* knowing *v. More precisely, v is the image of 1 under a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L_{(I,w)}$, and $w = v\overline{v}$ if and only if $\langle av, bv\rangle_{I,w} = t(a\overline{b}) = \langle a, b\rangle_{\mathbb{Z}\langle G\rangle}$ for all $a, b \in \mathbb{Z}\langle G\rangle$. Thus, finding v from I and $v\overline{v}$ in polynomial time is equivalent to finding a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L_{(I,w)}$ in polynomial time.*

The point of dividing by w in the definition of $\langle x, y\rangle_{I,w}$ is to make the lattice L unimodular. It follows that when we take tensor powers of L over $\mathbb{Z}\langle G\rangle$, as we will do in §3 below, there will be no coefficient blow-up.

We next show how to recover the Gentry-Szydlo result from Theorem 1.1. The Gentry-Szydlo algorithm finds a generator v of an ideal I of finite index in the ring $R = \mathbb{Z}[X]/(X^n - 1)$, given $v\overline{v}$, a $\mathbb{Z}$-basis for I, and a "promise" that v exists. Here, n is an odd prime, and for $v = v(X) = \sum_{i=0}^{n-1} a_i X^i \in R$, its "reversal" is $\overline{v} = v(X^{-1}) = a_0 + \sum_{i=1}^{n-1} a_{n-i} X^i \in R$. We take G to be a cyclic group of order $2n$. Then $R \cong \mathbb{Z}\langle G\rangle$ as in Example 2.16, and we identify R with $\mathbb{Z}\langle G\rangle$. Let $w = v\overline{v} \in \mathbb{Z}\langle G\rangle$ and let $L = L_{(I,w)}$ as above. Then L is the "implicit orthogonal lattice" in §7.2 of [6]. Once you know a $\mathbb{Z}$-basis for I and w, you know L. Theorem 1.1 produces a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ in polynomial time, and thus gives a generator v in polynomial time.

3 Invertible G-lattices, short vectors, and the tensor algebra Λ

In this section we give some concepts that we will use to prove Theorem 1.1.

3.1 Invertible G-lattices

Definition 3.1 *If L is a G-lattice, then the G-lattice $\overline{L}$ is a lattice equipped with a lattice isomorphism $L \xrightarrow{\sim} \overline{L}$, $x \mapsto \overline{x}$ and a group homomorphism $G \to \mathrm{Aut}(\overline{L})$ defined by $\sigma\overline{x} = \overline{\sigma^{-1}x} = \overline{\sigma}\,\overline{x}$ for all $\sigma \in G$ and $x \in L$, i.e., $\overline{\sigma x} = \overline{\sigma}\,\overline{x}$.*

Definition 3.2 *If L is a G-lattice, define the lifted inner product*

$$\cdot : L \times \overline{L} \to \mathbb{Z}\langle G\rangle \quad by \quad x \cdot \overline{y} = \sum_{\sigma \in S} \langle x, \sigma y\rangle \sigma \in \mathbb{Z}\langle G\rangle.$$

Then

$$\langle x, y\rangle = t(x \cdot \overline{y}) \tag{1}$$

and $x \cdot \overline{y} = \overline{y \cdot \overline{x}}$. This lifted inner product is $\mathbb{Z}\langle G\rangle$-bilinear, i.e., $(ax) \cdot \overline{y} = x \cdot (a\overline{y}) = a(x \cdot \overline{y})$ for all $a \in \mathbb{Z}\langle G\rangle$ and all $x, y \in L$.

Example 3.3 *If $L = \mathbb{Z}\langle G\rangle$, then $\overline{L} = \mathbb{Z}\langle G\rangle$ with $^-$ having the same meaning as in Definition 2.10 for $A = \mathbb{Z}$, and with $\cdot$ being multiplication in $\mathbb{Z}\langle G\rangle$.*

Definition 3.4 *A G-lattice L is* **invertible** *if the following three conditions all hold:*

(i) $\mathrm{rank}(L) = n = |G|/2$;
(ii) *L is unimodular (see Definition 2.3);*
(iii) *for each $m \in \mathbb{Z}_{>0}$ there exists $e_m \in L$ such that $\{\sigma e_m + mL : \sigma \in G\}$ generates the abelian group L/mL.*

Example 3.5 *If a G-lattice L is G-isomorphic to the standard G-lattice then L is invertible. For (iii), observe that the group $\mathbb{Z}\langle G\rangle$ is generated by $\{\sigma 1 : \sigma \in G\}$, so the group L is generated by $\{\sigma e : \sigma \in G\}$ where e is the image of 1 under the isomorphism. Now let $e_m = e$ for all m.*

Remark 3.6 *In the full version of the paper we will show that a G-lattice L is invertible if and only if there is a $\mathbb{Z}\langle G\rangle$-module M such that $L \otimes_{\mathbb{Z}\langle G\rangle} M$ and $\mathbb{Z}\langle G\rangle$ are isomorphic as $\mathbb{Z}\langle G\rangle$-modules and L is unimodular. (See Chapter XVI of [8] for tensor products.) We will also show that this is equivalent to the map $\varphi : L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} \to \mathbb{Z}\langle G\rangle$ defined by $\varphi(x \otimes \overline{y}) = x \cdot \overline{y}$ being an isomorphism of $\mathbb{Z}\langle G\rangle$-modules. Further, L is invertible if and only if L is G-isomorphic to $L_{(I,w)}$ for some I and w as in Example 2.18.*

Definition 3.4(iii) states that L/mL is a free $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$-module of rank one for all $m > 0$. Given an ideal, it is a hard problem to decide if it is principal. But checking (iii) of Definition 3.4 is easy algorithmically; see Proposition 4.4(ii) below.

3.2 Short vectors

Definition 3.7 *We will say that a vector e in an integral lattice L is* **short** *if $\langle e, e\rangle = 1$.*

Example 3.8 *The short vectors in the standard lattice of rank n are the $2n$ signed standard basis vectors $\{(0, \ldots, 0, \pm 1, 0, \ldots, 0)\}$. Thus, the set of short vectors in $\mathbb{Z}\langle G\rangle$ is G.*

Proposition 3.9 *Suppose L is an invertible G-lattice. Then:*

(i) *if e is short, then $\{\sigma \in G : \sigma e = e\} = \{1\}$;*
(ii) *if e is short, then $\langle e, \sigma e\rangle$ is 1 if $\sigma = 1$, is -1 if $\sigma = u$, and is 0 for all other $\sigma \in G$;*
(iii) *$e \in L$ is short if and only if $e \cdot \overline{e} = 1$, with inner product $\cdot$ defined in Definition 3.2.*

Proof. Suppose $e \in L$ is short. Let $H = \{\sigma \in G : \sigma e = e\}$. For all $\sigma \in G$, by the Cauchy-Schwarz inequality we have $|\langle e, \sigma e\rangle| \leq (\langle e, e\rangle\langle \sigma e, \sigma e\rangle)^{1/2} = \langle e, e\rangle = 1$, and $|\langle e, \sigma e\rangle| = 1$ if and only if e and σe lie on the same line through 0. Thus $\langle e, \sigma e\rangle \in \{1, 0, -1\}$. Then $\langle e, \sigma e\rangle = 1$ if and only if $\sigma \in H$. Also, $\langle e, \sigma e\rangle = -1$ if and only if $\sigma e = -e$ if and only if $\sigma \in Hu$. Otherwise, $\langle e, \sigma e\rangle = 0$. Thus for (i,ii), it suffices to prove $H = \{1\}$.

Let T be a set of coset representatives for G mod $H\langle u\rangle$ and let $S = T \cdot H$, a set of coset representatives for G mod $\langle u\rangle$. If $a = \sum_{\sigma\in S} a_\sigma \sigma \in (\mathbb{Z}/m\mathbb{Z})\langle G\rangle$ is fixed by H, then $a_{\tau\sigma} = a_\sigma$ for all $\sigma \in S$ and $\tau \in H$, so $a \in (\sum_{\tau\in H} \tau)(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$.

Let $m = |H|$. By Definition 3.4(iii), there is a $\mathbb{Z}[H]$-module isomorphism $L/mL \cong (\mathbb{Z}/m\mathbb{Z})\langle G\rangle$. The latter is a free module over $(\mathbb{Z}/m\mathbb{Z})[H]$ with basis T. Since $e + mL \in (L/mL)^H$ we have $e = m\varepsilon_1 + (\sum_{\tau\in H} \tau)\varepsilon_2$ with $\varepsilon_1, \varepsilon_2 \in L$. Since $\langle e, \tau\varepsilon_2\rangle = \langle \tau e, \tau\varepsilon_2\rangle = \langle e, \varepsilon_2\rangle$ for all $\tau \in H$, we have

$$1 = \langle e, e\rangle = m\langle e, \varepsilon_1\rangle + \sum_{\tau\in H} \langle e, \tau\varepsilon_2\rangle = m\langle e, \varepsilon_1 + \varepsilon_2\rangle \equiv 0 \mod m.$$

Thus, $m = 1$ as desired. Part (iii) follows directly from (ii) and Definition 3.2.

This enables us to prove the following result.

Proposition 3.10 *Suppose L is a G-lattice. Then:*

(i) *if L is invertible, then the map*

$$\{G\text{-isomorphisms } \mathbb{Z}\langle G\rangle \to L\} \to \{\text{short vectors of } L\}$$

that sends f to $f(1)$ is bijective;
(ii) *if $e \in L$ is short and L is invertible, then $\{\sigma e : \sigma \in G\}$ generates the abelian group L;*
(iii) *L is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if L is invertible and has a short vector;*
(iv) *if $e \in L$ is short and L is invertible, then the map $G \to \{\text{short vectors of } L\}$ defined by $\sigma \mapsto \sigma e$ is bijective.*

Proof. For (i), that $f(1)$ is short is clear. Injectivity of the map $f \mapsto f(1)$ follows from $\mathbb{Z}\langle G\rangle$-linearity of G-isomorphisms. For surjectivity, suppose $e \in L$ is short. Proposition 3.9(ii) says that $\{\sigma e\}_{\sigma\in S}$ is an orthonormal basis for L. Parts (ii) and (i)

now follow, where the G-isomorphism f is defined by $x \mapsto xe$ for all $x \in \mathbb{Z}\langle G\rangle$. Part (iii) follows from (i) and Example 3.5. For (iv), injectivity follows from Proposition 3.9(i). For surjectivity, suppose $e' \in L$ is short. Take G-isomorphisms f and f' with $f(1) = e$ and $f'(1) = e'$ as in (i), and let $\sigma = f^{-1} \circ f'(1)$. Then σ is a short vector in $\mathbb{Z}\langle G\rangle$ such that $\sigma e = e'$. By Example 3.8 we have $\sigma \in G$.

3.3 The Witt-Picard group

If L and M are invertible G-lattices, then the $\mathbb{Z}\langle G\rangle$-module $L \otimes_{\mathbb{Z}\langle G\rangle} M$ is a G-lattice with lifted inner product $(x \otimes v) \cdot (\overline{y} \otimes \overline{w}) = (x \cdot \overline{y})(v \cdot \overline{w})$, for all $x, y \in L$ and $v, w \in M$, and with lattice structure $\langle a, b\rangle = t(a \cdot \overline{b})$ for all $a, b \in L \otimes_{\mathbb{Z}\langle G\rangle} M$. In the notation of Example 2.18 we have

$$L_{(I_1,w_1)} \otimes_{\mathbb{Z}\langle G\rangle} L_{(I_2,w_2)} = L_{(I_1 I_2, w_1 w_2)},$$

where $I_1 I_2$ is the product of ideals.

Definition 3.11 *If L is an invertible G-lattice, let $[L]$ denote its G-isomorphism class, i.e., the class of all G-lattices that are G-isomorphic to L. We define the* **Witt-Picard group of** $\mathbb{Z}\langle G\rangle$ *to be the set of all G-isomorphism classes of invertible G-lattices, with group operation defined by $[L] \cdot [M] = [L \otimes_{\mathbb{Z}\langle G\rangle} M]$, with identity element $[\mathbb{Z}\langle G\rangle]$, and with $[L]^{-1} = [\overline{L}]$.*

The Witt-Picard group is a finite abelian group. When computing in the Witt-Picard group, one can apply a lattice basis reduction algorithm whenever the numbers get too large. More precisely, algorithmically we represent an invertible G-lattice M by letting $M = \mathbb{Z}^n$ as an abelian group, specifying a group homomorphism $G \to \mathrm{GL}(n, \mathbb{Z})$ giving the action of G on M, and giving data describing the map $\cdot : M \times \overline{M} \to \mathbb{Z}\langle G\rangle$; the lattice structure is then given by $\langle a, b\rangle = t(a \cdot \overline{b})$ for all $a, b \in M$. If M_1 and M_2 are invertible G-lattices, $m_1, m_2 \in \mathbb{Z}_{>0}$, and $d_i \in M_i/m_i M_i$ for $i = 1, 2$, one can compute $(M_1 \otimes_{\mathbb{Z}\langle G\rangle} M_2, d_1 \otimes d_2)$ in polynomial time. Also, there is a deterministic polynomial time algorithm that, given M and given $d \in M/mM$, produces a pair (M', d') and a G-isomorphism $(M, d) \to (M', d')$ such that the standard basis of $M' = \mathbb{Z}^n$ is LLL-reduced (and thus each entry of the Gram matrix is at most 2^{n-1} in absolute value, by Lemma 3.12 below). This in fact proves the finiteness of the Witt-Picard group.

If $L = L_{(I,w)}$ for some I and w as in Example 2.18, and $j \in \mathbb{Z}_{>0}$, then $[L]^j$ is the G-isomorphism class of $L_{(I^j, w^j)}$. One can compute $[L]^j$ in deterministic polynomial time using an addition chain for j, and LLL-reducing intermediate powers to prevent coefficient blow-up. This takes the place of the polynomial chains in §7.4 of [6].

Lemma 3.12 *If $\{b_1, \ldots, b_n\}$ is an LLL-reduced basis for an integral unimodular lattice L and $\{b_1^*, \ldots, b_n^*\}$ is its Gram-Schmidt orthogonalization, then*

$$2^{1-i} \leq |b_i^*|^2 \leq 2^{n-i}$$

and $|b_i|^2 \le 2^{n-1}$ *for all* $i \in \{1, \dots, n\}$.

Proof. Being LLL-reduced means that $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*$ with $|\mu_{ij}| \le \frac{1}{2}$ for all $j < i \le n$, and $|b_i^*|^2 \le 2|b_{i+1}^*|^2$ for all $i < n$. Thus for $1 \le j \le i \le n$ we have $|b_i^*|^2 \le 2^{j-i}|b_j^*|^2$, so for all i we have

$$2^{1-i}|b_1^*|^2 \le |b_i^*|^2 \le 2^{n-i}|b_n^*|^2.$$

Since L is integral we have $|b_1^*|^2 = |b_1|^2 = \langle b_1, b_1 \rangle \ge 1$, so $|b_i^*|^2 \ge 2^{1-i}$. Letting $L_i = \sum_{j=1}^{i} \mathbb{Z} b_j$, then $|b_i^*| = \det(L_i)/\det(L_{i-1})$. Since L is integral and unimodular, $|b_n^*| = \det(L_n)/\det(L_{n-1}) = 1/\det(L_{n-1}) \le 1$, so $|b_i^*|^2 \le 2^{n-i}$. Since $\{b_i^*\}$ is orthogonal we have

$$\begin{aligned} |b_i|^2 = |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2 &\le 2^{n-i} + \frac{1}{4} \sum_{j=1}^{i-1} 2^{n-j} \\ &= 2^{n-i} + (2^{n-2} - 2^{n-i-1}) = 2^{n-2} + 2^{n-i-1} \le 2^{n-1}. \end{aligned}$$

3.4 The extended tensor algebra Λ

We are now ready to introduce the extended tensor algebra Λ in which our computations take place. Suppose L is an invertible G-lattice. Letting $L^{\otimes 0} = \mathbb{Z}\langle G \rangle$ and letting $L^{\otimes m} = L \otimes_{\mathbb{Z}\langle G \rangle} \cdots \otimes_{\mathbb{Z}\langle G \rangle} L$ (m times) and $L^{\otimes(-m)} = \overline{L}^{\otimes m} = \overline{L} \otimes_{\mathbb{Z}\langle G \rangle} \cdots \otimes_{\mathbb{Z}\langle G \rangle} \overline{L}$ for all $m \in \mathbb{Z}_{>0}$, define the extended tensor algebra

$$\Lambda \;=\; \bigoplus_{i \in \mathbb{Z}} L^{\otimes i} \;=\; \dots \oplus \overline{L}^{\otimes 3} \oplus \overline{L}^{\otimes 2} \oplus \overline{L} \oplus \mathbb{Z}\langle G \rangle \oplus L \oplus L^{\otimes 2} \oplus L^{\otimes 3} \oplus \dots$$

("extended" because we extend the usual notion to include negative exponents $L^{\otimes(-m)}$). Each $L^{\otimes i}$ is an invertible G-lattice, and represents $[L]^i$. For simplicity, we denote $L^{\otimes i}$ by L^i. The ring structure on Λ is defined as the ring structure on the tensor algebra, supplemented with the lifted inner product $\cdot$. The following result is straightforward.

Proposition 3.13 (i) *Λ is a commutative ring containing $\mathbb{Z}\langle G \rangle$ as a subring;*
(ii) *the action of G on L becomes multiplication in Λ, and likewise for the action of G on $\overline{L}$;*
(iii) *Λ has an involution $x \mapsto \overline{x}$ extending both the involution of $\mathbb{Z}\langle G \rangle$ and the map $L \xrightarrow{\sim} \overline{L}$;*
(iv) *the lifted inner product $\cdot : L \times \overline{L} \to \mathbb{Z}\langle G \rangle$ becomes multiplication in Λ;*
(v) *if $e \in L$ is short, then $\overline{e} = e^{-1}$ in Λ and $\Lambda = \mathbb{Z}\langle G \rangle[e, e^{-1}]$.*

All computations in Λ and in $\Lambda/m\Lambda$ will be done with homogeneous elements only, where the set of homogeneous elements of Λ is $\bigcup_{i \in \mathbb{Z}} L^i$.

4 The main ingredients

We give the main results that we will use to prove Theorem 1.1. Fix as before a finite abelian group G of order $2n$ and $u \in G$ of order 2. Let k denote the exponent of G. (The exponent of a group H is the least positive integer k such that $\sigma^k = 1$ for all $\sigma \in H$. The exponent of H divides $|H|$ and has the same prime factors as $|H|$.) For all $m \in \mathbb{Z}_{>1}$, denote by $k(m)$ the exponent of the unit group $(\mathbb{Z}\langle G\rangle/(m))^*$.

Remark 4.1 *By Proposition 3.10, the G-isomorphisms $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ are in one-to-one correspondence with the short vectors, and if a short $e \in L$ exists, then the short vectors of L are exactly the $2n$ vectors $\{\sigma e : \sigma \in G\}$. If k is the exponent of G, then $(\sigma e)^k = \sigma^k e^k = e^k$ in Λ. Hence for invertible L, all short vectors in L have the same k-th power $e^k \in \Lambda$. At least philosophically, it is easier to find things that are uniquely determined. We look for e^k first, and then recover e from it.*

Proposition 4.2 *There is a deterministic polynomial time algorithm that, given a finite commutative ring R and an R-module M, decides whether M is a free R-module of rank one, and if it is, finds a generator.*

Proof. We sketch a proof. A complete proof will be given in the full version of the paper.

The inputs are given as follows. The ring R is given as an abelian group (say, as a sum of cyclic groups) along with all the products of pairs of generators. The finite R-module M is given as an abelian group (say, as a sum of cyclic groups), and for all generators of the abelian group R and all generators of the abelian group M, we are given the module products in M.

If $\#M \neq \#R$, output "no" and stop.

Suppose that A and B are finite commutative rings, that $R \twoheadrightarrow A \times B$ is a surjective ring homomorphism with nilpotent kernel, and that $y_B \in M$ is such that the map $B \to M_B = B \otimes_R M$, $b \mapsto b \otimes y_B$ is an isomorphism. Let I denote the kernel of the natural map $R \to B$ and let N denote the image of IM under the natural map $M \to M_A$.

Initially, take $A = R$, $B = 0$, and $y_B = 0$. As long as $A \neq 0$, do the following. If $N = 0$, output "no" and stop. Otherwise, pick $x_A \in IM$ whose image $x \in N$ is nonzero. Compute $\boldsymbol{a} = \mathrm{Ann}_A x$, where Ann_A denotes the annihilator in A. Let $\boldsymbol{b} = \mathrm{Ann}_A \boldsymbol{a}$.

If $\boldsymbol{a} = \boldsymbol{a}^2$, then $A \xrightarrow{\sim} A/\boldsymbol{a} \times A/\boldsymbol{b}$ and $M_A \xrightarrow{\sim} M_{A/\boldsymbol{a}} \times M_{A/\boldsymbol{b}}$. The image of x is of the form $(x', 0)$. If x' does not generate $M_{A/\boldsymbol{a}}$, stop with "no". Otherwise, compute $\beta \in R$ that maps to $(0, 1)$ under the map $R \twoheadrightarrow A \times B$, and replace y_B, B, A by $\beta y_B + x_A$, $(A/\boldsymbol{a}) \times B$, $A/\boldsymbol{b}$, respectively. If $\boldsymbol{a} \neq \boldsymbol{a}^2$, then $\boldsymbol{a} \cap \boldsymbol{b}$ is a nonzero nilpotent ideal, and we replace A by $A/(\boldsymbol{a} \cap \boldsymbol{b})$ and leave y_B unchanged.

When $A = 0$, then I is nilpotent; say $I^r = 0$. Then $By = M_B = M/IM$ for $y = (y_B \mod IM)$. Thus,

$$M = Ry_B + IM = Ry_B + I(Ry_B + IM) = Ry_B + I^2M = \ldots = Ry_B + I^rM = Ry_B,$$

so output "yes".

Lemma 4.3 *Suppose that L is a G-lattice, $m \in \mathbb{Z}_{>0}$, and $e \in L$. Then*

$$\{\sigma e + mL : \sigma \in G\}$$

generates L/mL as an abelian group if and only if $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is finite of order coprime to m.

Proof. The set $\{\sigma e + mL : \sigma \in G\}$ generates L/mL as an abelian group if and only multiplication by m is onto as a map from $L/(\mathbb{Z}\langle G\rangle \cdot e)$ to itself. Since $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is a finitely generated abelian group, this holds if and only if $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is finite of order coprime to m.

Proposition 4.4 (i) *There is a deterministic polynomial time algorithm that, given G, a G-lattice L, and $m \in \mathbb{Z}_{>0}$, decides whether there exists $e_m \in L$ such that $\{\sigma e_m + mL : \sigma \in G\}$ generates L/mL as an abelian group, and if so, finds one.*

(ii) *There is a deterministic polynomial time algorithm that, given G, u, and a G-lattice L, decides whether L is invertible.*

Proof. For (i), apply Proposition 4.2 with $R = \mathbb{Z}\langle G\rangle/(m)$ and $M = L/mL$.

For (ii), it is easy to check whether $\operatorname{rank}(L) = n$ and whether L is unimodular (check whether the Gram matrix has determinant 1). We need to check Definition 3.4(iii) for all m's in polynomial time. We show that it suffices to check two particular values of m. First take $m = 2$, and use (i) to determine if e_2 exists. If not, output "no". If there is one, use (i) to compute $e_2 \in L$. By Lemma 4.3, the group $L/(\mathbb{Z}\langle G\rangle \cdot e_2)$ is finite of odd order. Let q denote its order. Now apply (i) with $m = q$. If no e_q exists, output "no". If e_q exists, then for *all* $m \in \mathbb{Z}_{>0}$ there exists $e_m \in L$ that generates L/mL as a $\mathbb{Z}\langle G\rangle/(m)$-module, as follows. We can reduce to m being a prime power p^t, since if $\gcd(m, m') = 1$ then $L/mm'L$ is free of rank one over $\mathbb{Z}\langle G\rangle/(mm')$ if and only if L/mL is free of rank one over $\mathbb{Z}\langle G\rangle/(m)$ and $L/m'L$ is free of rank one over $\mathbb{Z}\langle G\rangle/(m')$. Lemma 4.3 now allows us to reduce to the case $m = p$. If $p \nmid q$, we can take $e_p = e_2$. If $p \mid q$, we can take $e_p = e_q$.

Proposition 4.5 *There is a deterministic polynomial time algorithm that, given a finite abelian group G of order $2n$ and $u \in G$ of order 2, determines prime powers ℓ and m such that $\ell, m \geq 2^{n/2} + 1$ and $\gcd(k(\ell), k(m)) = k$.*

Proof. One can prove that if p is prime and $p \equiv 1 \bmod k$, then

$$k(p^j) = (p-1)p^{j-1},$$

using induction on j and the facts that $(\mathbb{Z}\langle G\rangle/(p^j))^* \supset (\mathbb{Z}/p^j\mathbb{Z})^*$ and the latter group has exponent $(p-1)p^{j-1}$.

We next give an algorithm that, given $n, k \in \mathbb{Z}_{>0}$ with k even, computes $r, s \in \mathbb{Z}_{>0}$ and primes p and q such that $p \equiv q \equiv 1 \bmod k$,

$$\gcd((p-1)p^{r-1}, (q-1)q^{s-1}) = k,$$

$p^r \geq 2^{n/2}+1$, and $q^s \geq 2^{n/2}+1$. (We can then take $\ell = p^r$ and $m = q^s$.) Try $p = k+1, 2k+1, 3k+1, \ldots$ until the smallest prime $p \equiv 1 \bmod k$ is found. Find the least r such that $p^r \geq 2^{n/2}+1$. Try $q = p+k, p+2k, \ldots$ until the least prime $q \equiv 1 \bmod k$ such that $\gcd((p-1)p, q-1) = k$ is found. Find the smallest s such that $q^s \geq 2^{n/2}+1$.

This algorithm terminates, with correct output, in time $(n+k)^{O(1)}$. The key ingredient for proving this is Heath-Brown's version of Linnik's theorem [7], which implies that the prime p found by the algorithm satisfies $p \leq ck^{5.5}$ with an effective constant c. If $p-1 = k_1k_2$ with every prime divisor of k_1 also dividing k and with $\gcd(k_2, k) = 1$, then to have $\gcd((p-1)p, q-1) = k$ it suffices to have $q \equiv 2 \bmod p$ and $q \equiv 1+k \bmod k_1$ and $q \equiv 2 \bmod k_2$. This gives a congruence $q \equiv a \bmod p(p-1)$ for some a. Heath-Brown's version of Linnik's theorem implies that $q \leq c(p^2)^{5.5} \leq c^{12}k^{60.5}$.

Our prime powers ℓ and m play the roles that in the Gentry-Szydlo paper [6] were played by auxiliary prime numbers $P, P' > 2^{(n+1)/2}$ such that

$$\gcd(P-1, P'-1) = 2n.$$

Our $k(\ell)$ and $k(m)$ replace their $P-1$ and $P'-1$, respectively. While the Gentry-Szydlo primes P and P' are found with at best a probabilistic algorithm, we can find ℓ and m in deterministic polynomial time. (Further, the ring elements they work with were required to not be zero divisors modulo P, P' and other small auxiliary primes; we require no analogous condition on ℓ and m, since by Definition 3.4(iii), when L is invertible then for *all* m, the $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$-module L/mL is free of rank one.)

Proposition 4.6 (i) *Suppose L is an integral lattice, $3 \leq m \in \mathbb{Z}$, and $C \in L/mL$. Then C contains at most one element x with $\langle x, x\rangle = 1$.*

(ii) *There is a deterministic polynomial time algorithm that, given a rank n integral lattice L, $m \in \mathbb{Z}$ such that $m \geq 2^{n/2}+1$, and $C \in L/mL$, finds all $x \in C$ with $\langle x, x\rangle = 1$ (and the number of them is 0 or 1).*

Proof. For (i), suppose $x, y \in C$, $\langle x, x\rangle = \langle y, y\rangle = 1$, and $x \neq y$. Since $x - y \in mL$ and L is an integral lattice, we have

$$m \leq \langle x - y, x - y\rangle^{1/2} \leq \langle x, x\rangle^{1/2} + \langle y, y\rangle^{1/2} = 1 + 1 = 2$$

by the triangle inequality. This contradicts $m \geq 3$, giving (i).

For (ii), using LLL to solve the closest vector problem, one can find (in polynomial time) $y \in C$ such that $\langle y, y\rangle < (2^n - 1)\langle x, x\rangle$ for all $x \in C$. Suppose $x \in C$ with $\langle x, x\rangle = 1$. Since $x, y \in C$, there exists $w \in L$ such that $x - y = mw$. Then

$$m\langle w, w\rangle^{1/2} = \langle x - y, x - y\rangle^{1/2} \leq \langle x, x\rangle^{1/2} + \langle y, y\rangle^{1/2} < (1 + 2^{n/2})\langle x, x\rangle^{1/2} \leq m.$$

Therefore $1 > \langle w, w\rangle^{1/2} \in \mathbb{Z}$, so $w = 0$, and thus $y = x$. Compute $\langle y, y\rangle$. If $\langle y, y\rangle = 1$, output y. If $\langle y, y\rangle \neq 1$, there is no $x \in C$ with $\langle x, x\rangle = 1$.

The n of [6] is an odd prime, so $k = 2n$ and $\mathbb{Z}\langle G\rangle$ embeds in $\mathbb{Q}(\zeta_n) \times \mathbb{Q}$. Since the latter is a product of only two number fields, the number of zeros of $X^{2n} - v^{2n}$ is at most $(2n)^2$, and the Gentry-Szydlo method for finding v from v^{2n} is sufficiently efficient. If one wants to generalize [6] to the case where n is not prime, then the smallest t such that $\mathbb{Z}\langle G\rangle$ embeds in $F_1 \times \ldots \times F_t$ with number fields F_i can be large. Given ν, the number of zeros of $X^k - \nu$ could be as large as k^t. Finding e such that $\nu = e^k$ then requires a more efficient algorithm, which we attain with Proposition 4.9 below.

An **order** is a commutative ring A whose additive group is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$. We specify an order by saying how to multiply any two vectors in a given basis. Let $\mu(A)$ denote the group of roots of unity in A.

Proposition 4.7 *There is a deterministic polynomial time algorithm that, given an order A, determines a set of generators for $\mu(A)$.*

Proof. The proof is a bit intricate, involving commutative algebra and algorithmic algebraic number theory. We give a sketch. See [1] for commutative algebra background.

One starts by computing the nilradical N of the $\mathbb{Q}$-algebra $A_{\mathbb{Q}} = A \otimes_{\mathbb{Z}} \mathbb{Q}$ as well as the unique subalgebra $E \subset A_{\mathbb{Q}}$ that maps isomorphically to $A_{\mathbb{Q}}/N$. One has $\mu(A) \subset E$, so replacing A by $A \cap E$ one reduces to the case in which the nilradical of A is 0, which we now assume. Next one determines the set $\mathrm{Spec}(E)$ of prime ideals $\mathfrak{m}$ of E. For each $\mathfrak{m}$ we compute $E/\mathfrak{m}$, which is an algebraic number field, and we also compute its subring $A/(\mathfrak{m} \cap A)$. One has $E \cong \prod_{\mathfrak{m} \in \mathrm{Spec}(E)} E/\mathfrak{m}$, and we identify A with a subring of finite additive index in the product ring $B = \prod_{\mathfrak{m} \in \mathrm{Spec}(E)} A/(\mathfrak{m} \cap A)$.

For each prime number p dividing $|\mu(A)|$ one has $p \leq 1 + \dim_{\mathbb{Q}} E$, so it will suffice to find, for each such p, a set of generators for the p-primary component $\mu(A)_p$ of $\mu(A)$. Fix now a prime number $p \leq 1 + \dim_{\mathbb{Q}} E$.

Since each $A/(\mathfrak{m} \cap A)$ is contained in a number field, $\mu(A/(\mathfrak{m} \cap A))_p$ is cyclic and easy to determine. This leads to a set of generators for $\mu(B)_p$.

Compute $C = \{x \in B : p^i x \in A \text{ for some } i \in \mathbb{Z}_{\geq 0}\}$; this is a subring of B containing A. The group C/A is finite of p-power order, and the group B/C is finite of order not divisible by p. We make $\mathrm{Spec}(E)$ into the set of vertices of a graph by connecting $\mathfrak{m}, \mathfrak{n} \in \mathrm{Spec}(E)$ with an edge if and only if

$$(\mathfrak{m} \cap C) + (\mathfrak{n} \cap C) \neq C.$$

For each connected component V of this graph, determine the image C_V of C in the product ring $\prod_{\mathfrak{m} \in V} A/(\mathfrak{m} \cap A)$. Then one can show that one has $C \cong \prod_V C_V$, with V ranging over the connected components, so that $\mu(C)_p \cong \prod_V \mu(C_V)_p$. In addition, one can show that for each V and each $\mathfrak{m} \in V$ the natural map $\mu(C_V)_p \to \mu(A/(\mathfrak{m} \cap A))_p$ is *injective*, so that $\mu(C_V)_p$ is cyclic; the proof also leads to an efficient algorithm for computing $\mu(C_V)_p$. Thus, at this point one knows a set of generators for $\mu(C)_p$.

To pass from $\mu(C)_p$ to $\mu(A)_p$, one starts by computing the intersection $\mathbf{r}$ of all maximal ideals of C that contain p, as well as $\mathbf{s} = \mathbf{r} \cap A$. One has $\mu(C)_p \subset 1 + \mathbf{r}$ and $\mu(A)_p = \mu(C)_p \cap (1 + \mathbf{s})$. To compute the latter intersection, one determines $t \in \mathbb{Z}_{>0}$ with $p^t C \subset A$ as well as a presentation for the finite abelian p-group $1 + (\mathbf{r}/p^t C)$, which is a subgroup of the unit group $(C/p^t C)^*$; to do this, one uses that $\mathbf{r}/p^t C$ is a nilpotent ideal of $C/p^t C$. The group $\mu(A)_p$ is now obtained as the kernel of the natural map $\mu(C)_p \to (1 + (\mathbf{r}/p^t C))/(1 + (\mathbf{s}/p^t C))$.

Proposition 4.8 *Suppose L is an invertible G-lattice, $r \in \mathbb{Z}_{>0}$, and ν is a short vector in the G-lattice L^r. Let $A = \Lambda/(\nu - 1)$. Identifying $\bigoplus_{i=0}^{r-1} L^i \subset \Lambda$ with its image in A, we can view $A = \bigoplus_{i=0}^{r-1} L^i$ as a $\mathbb{Z}/r\mathbb{Z}$-graded ring. Then:*

(i) $G \subseteq \mu(A) \subseteq \bigcup_{i=0}^{r-1} L^i$,
(ii) $\{e \in L : e \cdot \bar{e} = 1\} = \mu(A) \cap L$,
(iii) $|\mu(A)|$ *is divisible by* $2n$ *and divides* $2nr$, *and*
(iv) *there exists* $e \in L$ *for which* $e \cdot \bar{e} = 1$ *if and only if* $|\mu(A)| = 2nr$.

Proof. Since the ideal $(\overline{\nu} - 1) = (\nu^{-1} - 1) = (1 - \nu) = (\nu - 1)$, the map $a \mapsto \overline{a}$ induces an involution on A. Since the lattice's inner product is symmetric and positive definite, for all ring homomorphisms $\psi : A \to \mathbb{C}$ we have $\overline{(a)} = \overline{\psi(a)}$ for all $a \in A$, and $\bigcap \ker \psi = 0$. Let $E = \{e \in A : e\overline{e} = 1\}$, a subgroup of A^*.

Suppose $e \in \mu(A)$. Then for all ring homomorphisms $\psi : A \to \mathbb{C}$ we have $1 = (e)\overline{\psi(e)} = \psi(e)\psi(\overline{e}) = \psi(e\overline{e})$, so $e\overline{e} = 1$. Thus, $\mu(A) \subseteq E$.

Conversely, suppose $e \in E$. Write $e = \sum_{i=0}^{r-1} \varepsilon_i$ with $\varepsilon_i \in L^i$, so $\overline{e} = \sum_{i=0}^{r-1} \overline{\varepsilon}_i$ with $\overline{\varepsilon}_i \in L^{-i} = L^{r-i}$ in A. We have $1 = e\overline{e} = \sum_{i=0}^{r-1} \varepsilon_i \overline{\varepsilon}_i$ (the degree 0 piece of $e\overline{e}$). Applying the map t of Definition 2.9 and using (1) we have $1 = \sum_{i=0}^{r-1} \langle \varepsilon_i, \varepsilon_i \rangle$. It follows that there exists j such that $\langle \varepsilon_j, \varepsilon_j \rangle = 1$, and $\varepsilon_i = 0$ if $i \neq j$. Thus,

$E \subseteq \bigcup_{i=0}^{r-1}\{e \in L^i : \langle e, e\rangle = 1\}$, giving (i). By Proposition 3.9(iii) and Example 3.8 we have $E \cap \mathbb{Z}\langle G\rangle = G$, so $\mu(\mathbb{Z}\langle G\rangle) = G$.

The degree map from E to $\mathbb{Z}/r\mathbb{Z}$ that takes $e \in E$ to j such that $e \in L^j$ is a group homomorphism with kernel $E \cap \mathbb{Z}\langle G\rangle = G$. Therefore, $|E|$ divides $|G| \cdot |\mathbb{Z}/r\mathbb{Z}| = 2nr$. Thus, $E \subseteq \mu(A) \subseteq E$, so $E = \mu(A)$ and we have (ii,iii). The degree map is surjective if and only if $|\mu(A)| = 2nr$, and if and only if 1 is in the image, i.e., if and only if $\mu(A) \cap L \neq \emptyset$. Part (iv) now follows from (ii).

Proposition 4.9 *There is a deterministic polynomial time algorithm that, given G of exponent k, an invertible G-lattice L, and $\nu \in L^k$, determines whether there exists $e \in L$ such that $\nu = e^k$ and $e \cdot \bar{e} = 1$, and if so, finds one.*

Proof. Check whether $\nu\overline{\nu} = 1$. If so, let $A = \Lambda/(\nu - 1)$ and apply Proposition 4.7 to compute generators for $\mu(A)$. Using Proposition 4.8 with $r = k$, apply the degree map $\mu(A) \to \mathbb{Z}/k\mathbb{Z}$ to the generators, check whether the images generate $\mathbb{Z}/k\mathbb{Z}$, and if they do, compute an element $e \in \mu(A)$ whose image is 1. Then $e \in \mu(A) \cap L = \{e \in L : e \cdot \bar{e} = 1\}$. Check whether $\nu = e^k$. If any step fails, no such e exists (by Remark 4.1). The algorithm runs in polynomial time since $2nk \leq (2n)^2$.

5 The Algorithm

We present the main algorithm, followed by a fuller explanation. As before, k is the exponent of the group G and $k(j)$ is the exponent of $(\mathbb{Z}\langle G\rangle/(j))^*$ if $j \in \mathbb{Z}_{>1}$.

Algorithm 5.1 *Input a finite abelian group G, an element $u \in G$ of order 2, and a G-lattice L. Output a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$, or a proof that none exists.*

(i) *Apply Proposition 4.4(ii) to check whether L is invertible. If it is not, terminate with "no".*
(ii) *Find ℓ and m as in Proposition 4.5.*
(iii) *Compute $e_{\ell m}$ as in Proposition 4.4(i).*
(iv) *Using an addition chain for $k(m)$ and the algorithms mentioned in §3.3, compute the pair $(L^{k(m)}, e_{\ell m}^{k(m)} + mL^{k(m)})$. Use Proposition 4.6(ii) to decide whether the coset $e_{\ell m}^{k(m)} + mL^{k(m)}$ contains a short vector $\nu_m \in L^{k(m)}$, and if so, compute it. Terminate with "no" if none exists.*
(v) *Compute $s \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$ such that*

$$\nu_m = s(e_{\ell m}^{k(m)} + \ell L^{k(m)})$$

in $L^{k(m)}/\ell L^{k(m)}$.
(vi) *Use the extended Euclidean algorithm to find $b \in \mathbb{Z}$ such that*

$$bk(m) \equiv k \mod k(\ell).$$

(vii) *Using an addition chain for k and the algorithms mentioned in §3.3, compute the pair $(L^k, e_{\ell m}^k + \ell L^k)$ and compute $s^b(e_{\ell m}^k + \ell L^k)$. Use Proposition 4.6(ii) to decide whether the latter coset contains a short vector $\nu \in L^k$, and if so, compute it. Terminate with "no" if none exists.*

(viii) *Apply Proposition 4.9 to find $e \in L$ such that $\nu = e^k$ and $e \cdot \bar{e} = 1$ (or to prove there is no G-isomorphism).*

We explain the algorithm in more detail. By Proposition 3.10(iii), the G-lattice L is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if L is invertible and has a short vector. Run the algorithm in Proposition 4.4(ii) to check whether L is invertible. If it is not, terminate with "no". If it is, we look for an $e \in L$ such that $e\bar{e} = 1$. Lattice basis reduction algorithms such as LLL can find fairly short vectors, but they are not nearly short enough for our purpose. We supplement LLL with computations modulo m. Any short e satisfies $\mathbb{Z}\langle G\rangle e = L$, which implies that for all $m \in \mathbb{Z}_{>0}$, the coset $e + mL$ generates L/mL as a $\mathbb{Z}\langle G\rangle/(m)$-module. Proposition 4.4(i) gives another generator e_m. Thus, $e_m = ye$ for some $y \in (\mathbb{Z}\langle G\rangle/(m))^*$. We have $e_m^{k(m)} \bmod m = e^{k(m)} \bmod m$ in $\Lambda/m\Lambda$.

Apply Proposition 4.5 to find prime powers $m, \ell \geq 2^{n/2} + 1$ such that

$$\gcd(k(\ell), k(m)) = k.$$

Compute $e_{\ell m}$ (which works as both e_m and e_ℓ) as in Proposition 4.4(i). Proposition 4.6(ii) applied to the coset $e_{\ell m} + mL^{k(m)} \in L^{k(m)}/mL^{k(m)}$ finds a short vector ν_m (if it exists). If $e \in L$ is short, then $\nu_m = e^{k(m)}$ by Proposition 4.6(i).

Since $e_{\ell m}^{k(m)}$ (by definition) and ν_m (by Proposition 3.10(ii)) each generate the $(\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle$-module $L^{k(m)}/\ell L^{k(m)}$, we can find $s \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$ such that $\nu_m = s(e_{\ell m}^{k(m)} + \ell L^{k(m)})$ in $L^{k(m)}/\ell L^{k(m)}$. Since $k = \gcd(k(\ell), k(m))$, we can use the extended Euclidean algorithm to find $a, b \in \mathbb{Z}$ such that $ak(\ell) + bk(m) = k$. Compute $s^b \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$ and $s^b e_{\ell m}^k \in L^k/\ell L^k$ and use Proposition 4.6(ii) to compute a short $\nu \in L^k$ in this coset or prove that none exists. If $e \in L$ is short, then $e^{k(m)} = \nu_m \equiv s e_{\ell m}^{k(m)} \bmod \ell\Lambda$, so $e^k \equiv \nu_m^b (e_{\ell m}^{k(\ell)})^a \equiv s^b e_{\ell m}^k \bmod \ell\Lambda$, so $s^b(e_{\ell m}^k + \ell L^k)$ contains the short vector e^k of L^k, and by Proposition 4.6(i) we have $\nu = e^k$. Proposition 4.9 then finds a short vector $e \in L$, or proves none exists. The map $x \mapsto xe$ gives the desired G-isomorphism from $\mathbb{Z}\langle G\rangle$ to L. This completes the proof of Theorem 1.1.

Remark 5.2 *There is a version of the algorithm in which checking invertibility in step (i) is skipped. In this case, the algorithm may misbehave at other points, indicating that L is not invertible and thus not G-isomorphic to $\mathbb{Z}\langle G\rangle$. At the end one would check whether $\langle e, e\rangle = 1$ and $\langle e, \sigma e\rangle = 0$ for all $\sigma \neq 1, u$. If so, then $\{\sigma e\}_{\sigma \in S}$ is an orthonormal basis for L, and $x \mapsto xe$ gives the desired isomorphism; if not, no such isomorphism exists.*

Acknowledgments: We thank the participants of the August 2013 Workshop on Lattices with Symmetry, in particular Craig Gentry, René Schoof, and Mike Szydlo, and we thank the reviewers for helpful comments.

References

1. M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, MA, 1969.
2. S. Garg, C. Gentry, and S. Halevi, *Candidate multilinear maps from ideal lattices*, Advances in Cryptology—EUROCRYPT 2013, Lect. Notes in Comp. Sci. **7881**, Springer, 2013, 1–17.
3. C. Gentry, *Fully homomorphic encryption using ideal lattices*, in Proceedings of the 41st ACM Symposium on Theory of Computing—STOC 2009, ACM, New York (2009), 169–178.
4. C. Gentry, *A fully homomorphic encryption scheme*, Stanford University PhD thesis, 2009, `http://crypto.stanford.edu/craig/craig-thesis.pdf`.
5. C. Gentry, email, May 9, 2012.
6. C. Gentry and M. Szydlo, *Cryptanalysis of the revised NTRU signature scheme*, Advances in Cryptology—EUROCRYPT 2002, Lect. Notes in Comp. Sci. **2332**, Springer, Berlin, 2002, 299-320, full version at `http://www.szydlo.com/ntru-revised-full02.pdf`.
7. D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), 265–338.
8. S. Lang, Algebra, Third edition, Graduate Texts in Mathematics **211**, Springer-Verlag, New York, 2002.
9. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
10. H. W. Lenstra, Jr., *Lattices*, in Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press, Cambridge, 2008, 127–181.
11. N. Smart, personal communication.

DETERMINING CYCLICITY OF FINITE MODULES

H. W. LENSTRA, JR. AND A. SILVERBERG

Abstract. We present a deterministic polynomial-time algorithm that determines whether a finite module over a finite commutative ring is cyclic, and if it is, outputs a generator.

1. Introduction

If R is a commutative ring, then an R-module M is cyclic if there exists $y \in M$ such that $M = Ry$.

Theorem 1.1. *There is a deterministic polynomial-time algorithm that, given a finite commutative ring R and a finite R-module M, decides whether there exists $y \in M$ such that $M = Ry$, and if there is, finds such a y.*

We present the algorithm in Algorithm 4.1 below. The inputs are given as follows. The ring R is given as an abelian group by generators and relations, along with all the products of pairs of generators. The finite R-module M is given as an abelian group, and for all generators of the abelian groups R and all generators of the abelian group M we are given the module products in M.

Our algorithm depends on R being an Artin ring, and should generalize to finitely generated modules over any commutative Artin ring that is computationally accessible.

Theorem 1.1 is one of the ingredients of our work [4, 5] on lattices with symmetry, and a sketch of the proof is contained in [4]. Previously published algorithms of the same nature appear to restrict to rings that are algebras over fields. Subsequently to [4], I. Ciocănea-Teodorescu [2], using different and more elaborate techniques, greatly generalized our result, dropping the commutativity assumption on the finite ring R and finding, for any given finite R-module M, a set of generators for M of smallest possible size.

See Chapter 8 of [1] for commutative algebra background. For the purposes of this paper, commutative rings have an identity element 1, which may be 0.

Key words and phrases. algebraic algorithms, finite rings, cyclic modules.

This material is based on research sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750-13-2-0054 and by the Alfred P. Sloan Foundation. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

2. Lemmas on commutative rings

If R is a commutative ring and $\boldsymbol{a}$ is an ideal in R, let $\mathrm{Ann}_R\boldsymbol{a}$ denote the annihilator of $\boldsymbol{a}$ in R. We will use that every finite commutative ring is an Artin ring, that every Artin ring is isomorphic to a finite direct product of local Artin rings, and that the maximal ideal in a local Artin ring is always nilpotent.

Lemma 2.1. *If A is a local Artin ring, $\boldsymbol{a}$ is an ideal in A, and $\boldsymbol{a}^2 = \boldsymbol{a}$, then $\boldsymbol{a}$ is 0 or A.*

Proof. If $\boldsymbol{a}$ contains a unit, then $\boldsymbol{a} = A$. Otherwise, $\boldsymbol{a}$ is contained in the maximal ideal $\boldsymbol{m}$, which is nilpotent. Thus there is an $r \in \mathbb{Z}_{>0}$ such that $\boldsymbol{m}^r = 0$. Now $\boldsymbol{a} = \boldsymbol{a}^2 = \cdots = \boldsymbol{a}^r \subset \boldsymbol{m}^r = 0$. □

Lemma 2.2. *Suppose that A is a finite commutative ring, $\boldsymbol{a}$ is an ideal in A, $\boldsymbol{b} = \mathrm{Ann}_A\boldsymbol{a}$, and $\boldsymbol{a} \cap \boldsymbol{b} = 0$. Then:*

(i) $\boldsymbol{a}^2 = \boldsymbol{a}$;
(ii) *there is an idempotent $e \in A$ such that $\boldsymbol{a} = eA$, $\boldsymbol{b} = (1-e)A$, and $A = (1-e)A \oplus eA = \boldsymbol{b} \oplus \boldsymbol{a}$;*
(iii) *if $\boldsymbol{b} = 0$ then $\boldsymbol{a} = A$.*

Proof. Write A as a finite direct product of local Artin rings $A_1 \times \cdots \times A_s$. Then $\boldsymbol{a}$ is a direct product $\boldsymbol{a}_1 \times \cdots \times \boldsymbol{a}_s$ of ideals $\boldsymbol{a}_i \subset A_i$. Assume $\boldsymbol{a}^2 \neq \boldsymbol{a}$. Then there is an i such that $\boldsymbol{a}_i^2 \neq \boldsymbol{a}_i$. Let $\boldsymbol{b}_i = \mathrm{Ann}_{A_i}\boldsymbol{a}_i$. Since $\boldsymbol{a} \cap \boldsymbol{b} = 0$, it follows that $\boldsymbol{a}_i \cap \boldsymbol{b}_i = 0$. Since A_i is a local ring, $\boldsymbol{a}_i$ is contained in the maximal ideal of A_i, so $\boldsymbol{a}_i$ is nilpotent. Let r denote the smallest positive integer such that $\boldsymbol{a}_i^r = 0$. Since $\boldsymbol{a}_i \neq 0$ we have $r \geq 2$. Then $\boldsymbol{a}_i^{r-1}$ is contained in $\boldsymbol{a}_i$ and kills $\boldsymbol{a}_i$, so $0 \neq \boldsymbol{a}_i^{r-1} \subset \boldsymbol{a}_i \cap \boldsymbol{b}_i = 0$, a contradiction. This gives (i).

Since A is a finite product of local Artin rings, $\boldsymbol{a}$ is generated by an idempotent e, by Lemma 2.1. Then $\boldsymbol{b} = (1-e)A$ and $A = (1-e)A \oplus eA = \boldsymbol{b} \oplus \boldsymbol{a}$. This gives (ii) and (iii). □

3. Preparatory lemmas

If R is a commutative ring, then a commutative R-algebra is a commutative ring A equipped with a ring homomorphism from R to A. Whenever A is an R-algebra, we let M_A denote the A-module $A \otimes_R M$.

From now on, suppose R is finite commutative ring and M is a finite R-module. Let $\mathcal{S}$ denote the set of quadruples (A, B, y, N) such that:

(i) A and B are finite commutative R-algebras for which the natural map $f : R \twoheadrightarrow A \times B$ is surjective and has nilpotent kernel,
(ii) $y \in M$ is such that the map $B \to M_B = B \otimes_R M$ defined by $b \mapsto b \otimes y$ is an isomorphism and such that $1 \otimes y = 0$ in M_A,
(iii) and N is a submodule of M such that the natural map $N \to M_A$ defined by $z \mapsto 1 \otimes z$ is onto and such that the natural map $N \to M_B$ is the zero map.

In Algorithm 4.1 below, initially we take $(A, B, y, N) = (R, 0, 0, M)$. Clearly, $(R, 0, 0, M) \in \mathcal{S}$. Throughout that algorithm, we always have $(A, B, y, N) \in \mathcal{S}$. While A and B occur in the proof of correctness of Algorithm 4.1, the R-algebra B does not actually occur in the algorithm itself.

Lemma 3.1. *If $(A, B, y, N) \in \mathcal{S}$ and $M_A = 0$, then $M = Ry$.*

Proof. Let J denote the kernel of $f : R \twoheadrightarrow A \times B$, and let I_A (resp., I_B) denote the kernel of the composition of f with projection from $A \times B$ onto A (resp., B). Since J is nilpotent we have $J^r = 0$ for some $r \in \mathbb{Z}_{>0}$. Since $0 = M_A = A \otimes_R M = (R/I_A) \otimes_R M \cong M/I_A M$ it follows that $I_A M = M$ Since $JM \subseteq I_B M = I_B I_A M \subseteq (I_B \cap I_A)M = JM$, it follows that $JM = I_B M$. Letting $y' = (y \mod I_B M) \in M/I_B M$, then $M_B \cong M/I_B M = By'$. Thus,

$$M = Ry + I_B M = Ry + JM = Ry + J(Ry + JM)$$
$$= Ry + J^2 M = \ldots = Ry + J^r M = Ry.$$

□

Lemma 3.2. *Suppose $(A, B, y, N) \in \mathcal{S}$ and $M_A \neq 0$. Then there exists $x \in N$ such that $1 \otimes x \neq 0$ in M_A. Choosing x and letting $\boldsymbol{a} = \mathrm{Ann}_A(1 \otimes x)$ and $\boldsymbol{b} = \mathrm{Ann}_A \boldsymbol{a}$, we have:*

(i) $(A/(\boldsymbol{a} \cap \boldsymbol{b}), B, y, N) \in \mathcal{S}$;
(ii) *If $\boldsymbol{a} \cap \boldsymbol{b} = 0$ and $(A/\boldsymbol{a}) \otimes x = M_{A/\boldsymbol{a}}$, then $(A/\boldsymbol{b}, (A/\boldsymbol{a}) \times B, x + y, \boldsymbol{a}N) \in \mathcal{S}$, where $\boldsymbol{a}N$ denotes $f^{-1}(\boldsymbol{a} \times B)N$.*
(iii) *If $\boldsymbol{a} \cap \boldsymbol{b} = 0$ and $(A/\boldsymbol{a}) \otimes x \neq M_{A/\boldsymbol{a}}$, then M is not cyclic.*

Proof. Since the map $N \to M_A$, $z \mapsto 1 \otimes z$ is onto, as long as $M_A \neq 0$ there exists $x \in N$ such that $1 \otimes x \neq 0$ in M_A.

Since $\boldsymbol{a}\boldsymbol{b} = 0$, we have $(\boldsymbol{a} \cap \boldsymbol{b})^2 = 0$, so $\boldsymbol{a} \cap \boldsymbol{b}$ is a nilpotent ideal in A. It follows that $(A/(\boldsymbol{a} \cap \boldsymbol{b}), B, y, N) \in \mathcal{S}$, giving (i).

From now on, suppose that $\boldsymbol{a} \cap \boldsymbol{b} = 0$. By Lemma 2.2, there is an idempotent $e \in A$ such that $\boldsymbol{a} = eA$, $\boldsymbol{b} = (1 - e)A$, and $A = (1 - e)A \oplus eA = \boldsymbol{b} \oplus \boldsymbol{a}$. It follows that $A \xrightarrow{\sim} A/\boldsymbol{a} \times A/\boldsymbol{b}$, so $M_A \xrightarrow{\sim} M_{A/\boldsymbol{a}} \times M_{A/\boldsymbol{b}}$. If (x', x'') is the image of $1 \otimes x$ under the latter map, then $x'' = 0$ (we have $\boldsymbol{b}x'' = 0$ since $x'' \in (A/\boldsymbol{b}) \otimes_R M$, and $\boldsymbol{a}x'' = 0$ since $\boldsymbol{a}(1 \otimes x) = 0$; thus $Ax'' = (\boldsymbol{a} + \boldsymbol{b})x'' = 0$, so $x'' = 0$). The map $i_{\boldsymbol{a}} : A/\boldsymbol{a} \to M_{A/\boldsymbol{a}}$ defined by $i_{\boldsymbol{a}}(t) = tx' = t \otimes x$ is injective since $\mathrm{Ann}_{A/\boldsymbol{a}} x' = 0$.

First suppose $(A/\boldsymbol{a}) \otimes x = M_{A/\boldsymbol{a}}$. Then the injective map $i_{\boldsymbol{a}}$ is an isomorphism. Since $0 = x'' = 1_{A/\boldsymbol{b}} \otimes x$, we have $1 \otimes (x + y) = 0$ in $M_{A/\boldsymbol{b}}$. It is now easy to check that $(A/\boldsymbol{b}, (A/\boldsymbol{a}) \times B, x + y, \boldsymbol{a}N) \in \mathcal{S}$, giving (ii). Note that $\boldsymbol{b} \neq 0$ (if $\boldsymbol{b} = 0$, then $\boldsymbol{a} = A$ by Lemma 2.2, contradicting that $1 \otimes x \neq 0$ in M_A).

Now suppose that $(A/\boldsymbol{a}) \otimes x \neq M_{A/\boldsymbol{a}}$. By way of contradiction, suppose M is a cyclic R-module. Then $M_{A/\boldsymbol{a}}$ is a cyclic $A/\boldsymbol{a}$-module. Since the domain and codomain of $i_{\boldsymbol{a}} : A/\boldsymbol{a} \hookrightarrow M_{A/\boldsymbol{a}}$ are both finite, it now follows that $i_{\boldsymbol{a}}$ is surjective, so $(A/\boldsymbol{a}) \otimes x = M_{A/\boldsymbol{a}}$. This contradiction gives (iii). □

The intuition behind Algorithm 4.1 is that throughout the algorithm, y generates the "non-A part" of M, and the goal is to shrink the "A-part" of M, namely N.

4. Main algorithm

Algorithm 4.1. Input a finite commutative ring R and a finite R-module M. Decide whether there exists $y \in M$ such that $M = Ry$, and if there is, find such a y.

(i) Initially, take $A = R$, $y = 0$, and $N = M$.
(ii) If $M_A = 0$, stop and output "yes" with generator y.
(iii) Otherwise, pick $x \in N$ such that $1 \otimes x \neq 0$ in M_A, and compute $\boldsymbol{a} = \mathrm{Ann}_A(1 \otimes x)$, $\boldsymbol{b} = \mathrm{Ann}_A \boldsymbol{a}$, and $\boldsymbol{a} \cap \boldsymbol{b}$.
(iv) If $\boldsymbol{a} \cap \boldsymbol{b} \neq 0$, replace A by $A/(\boldsymbol{a} \cap \boldsymbol{b})$ and go back to step (ii).
(v) If $\boldsymbol{a} \cap \boldsymbol{b} = 0$, then if $(A/\boldsymbol{a}) \otimes x \neq M_{A/\boldsymbol{a}}$ terminate with "no", and if $(A/\boldsymbol{a}) \otimes x = M_{A/\boldsymbol{a}}$ replace A, y, and N by $A/\boldsymbol{b}$, $x + y$, and $\boldsymbol{a}N$, respectively, and go back to step (ii).

Proposition 4.2. *Algorithm 4.1 runs in polynomial time, and on input a finite commutative ring R and a finite R-module M, decides whether there exists $y \in M$ such that $M = Ry$, and if there is, finds such a y.*

Proof. Since A is a finite ring, if the algorithm does not stop with "no" then eventually $A = 0$ and $M_A = 0$. Step (ii) of the algorithm is justified by Lemma 3.1, while steps (iii), (iv), and (v) are justified by Lemma 3.2.

The computations of annihilators and of the decompositions $A \xrightarrow{\sim} A/\boldsymbol{a} \times A/\boldsymbol{b}$ can be done in polynomial time using linear algebra (see §14 of [3]); in particular, $\boldsymbol{a}$ is the kernel of the map $A \to M_A$ defined by $t \mapsto t(1 \otimes x)$. For any B, compute M_B by computing $M/I_B M$ (and analogously for M_A). Each new A is at most half the size of the A it replaces. This implies that the number of steps is at most linear in the length of the input. □

References

[1] M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, MA, 1969.

[2] I. Ciocănea-Teodorescu, *The module isomorphism problem for finite rings and related results*, Abstract of a talk at the CAAFRTA session of the 20th Conference on Applications of Computer Algebra, July 10, 2014, `http://www.singacom.uva.es/~edgar/caafrta2014/files/Ciocanea.pdf`.

[3] H. W. Lenstra, Jr., *Lattices*, in Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press, Cambridge, 2008, 127–181.

[4] H. W. Lenstra, Jr. and A. Silverberg, *Revisiting the Gentry-Szydlo Algorithm*, in Advances in Cryptology—CRYPTO 2014, Lect. Notes in Comp. Sci. **8616**, Springer, Berlin, 2014, 280–296.

[5] H. W. Lenstra, Jr. and A. Silverberg, *Lattices with symmetry*, submitted.

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
E-mail address: hwl@math.leidenuniv.nl

Department of Mathematics, Rowland Hall, University of California, Irvine, CA 92697, USA
E-mail address: asilverb@uci.edu

LATTICES WITH SYMMETRY

H. W. LENSTRA, JR. AND A. SILVERBERG

Abstract. For large ranks, there is no good algorithm that decides whether a given lattice has an orthonormal basis. But when the lattice is given with enough symmetry, we can construct a provably deterministic polynomial-time algorithm to accomplish this, based on the work of Gentry and Szydlo. The techniques involve algorithmic algebraic number theory, analytic number theory, commutative algebra, and lattice basis reduction.

1. Introduction

Let G be a finite abelian group and let $u \in G$ be a fixed element of order 2. Define a G-lattice to be an integral lattice L with an action of G on L that preserves the inner product, such that u acts as -1. The *standard* G-lattice is the modified group ring $\mathbb{Z}\langle G\rangle = \mathbb{Z}[G]/(u+1)$, equipped with a natural inner product; we refer to Sections 2, 5, and 6 for more precise definitions. Our main result reads as follows:

Theorem 1.1. *There is a deterministic polynomial-time algorithm that, given a finite abelian group G with an element u of order 2, and a G-lattice L, decides whether L and $\mathbb{Z}\langle G\rangle$ are isomorphic as G-lattices, and if they are, exhibits such an isomorphism.*

We call a G-lattice L *invertible* if it is unimodular and there is a $\mathbb{Z}\langle G\rangle$-module M such that $L \otimes_{\mathbb{Z}\langle G\rangle} M$ and $\mathbb{Z}\langle G\rangle$ are isomorphic as $\mathbb{Z}\langle G\rangle$-modules (see Definition 9.5 and Theorem 11.1). For example, the standard G-lattice is invertible. The following result is a consequence of Theorem 1.1.

Theorem 1.2. *There is a deterministic polynomial-time algorithm that, given a finite abelian group G equipped with an element of order 2, and invertible G-lattices L and M, decides whether L and M are isomorphic as G-lattices, and if they are, exhibits such an isomorphism.*

Key words and phrases. lattices, Gentry-Szydlo algorithm, ideal lattices, lattice-based cryptography.

This material is based on research sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750-13-2-0054 and by the Alfred P. Sloan Foundation. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

We thank Craig Gentry, Daniele Micciancio, René Schoof, Mike Szydlo, and all the participants of the 2013 Workshop on Lattices with Symmetry. An extended abstract [7] appears in the Proceedings of Crypto 2014.

Deciding whether two lattices are isomorphic is a notorious problem. Our results show that it admits a satisfactory solution if the lattices are equipped with sufficient structure.

Our algorithms and runtime estimates draw upon an array of techniques from algorithmic algebraic number theory, commutative algebra, lattice basis reduction, and analytic number theory.

An important ingredient to our algorithm is a powerful novel technique that was invented by C. Gentry and M. Szydlo in Section 7 of [3]. We recast their method in the language of commutative algebra, replacing the "polynomial chains" that they used to compute powers of ideals in certain rings by tensor powers of modules. A number of additional changes enabled us to obtain a *deterministic* polynomial-time algorithm, whereas the Gentry-Szydlo algorithm is at best probabilistic.

The technique of Gentry and Szydlo has seen several applications in cryptography, as enumerated in [7]. By placing it in an algebraic framework, we have already been able to generalize the method significantly, replacing the rings $\mathbb{Z}[X]/(X^n - 1)$ (with n an odd prime) used by Gentry and Szydlo by the larger class of modified group rings that we defined above, and further extensions appear to be possible. In addition, we hope that our reformulation will make it easier to understand the method and improve upon it. This should help to make it more widely applicable in a cryptographic context.

The structure of the paper is as follows. Sections 2–4 contain background on integral lattices. In particular, we derive a new bound for the entries of a matrix describing an automorphism of a unimodular lattice with respect to a reduced basis (Proposition 3.4). Sections 5–7 contain basic material about G-lattices and modified group rings. Important examples of G-lattices are the ideal lattices introduced in Section 8. In Sections 9–11 we begin our study of invertible G-lattices, giving several equivalent definitions and an algorithm for recognizing invertibility. Section 12 is devoted to the following pleasing result: a G-lattice is G-isomorphic to the standard one if and only if it is invertible and has a vector of length 1. In Sections 13–14 we show how to multiply invertible G-lattices and we introduce the Witt-Picard group of $\mathbb{Z}\langle G\rangle$, of which the elements correspond to G-isomorphism classes of invertible G-lattices. It has properties reminiscent of the class group in algebraic number theory; in particular, it is a finite abelian group (Theorems 14.2 and 14.5). We also show how to do computations in the Witt-Picard group. In Section 15 we treat the extended tensor algebra Λ, which is in a sense the hero of story: it is a single algebraic structure that comprises all rings and lattices occurring in our main algorithm. Section 16 shows how Λ can be used to assist in finding vectors of length 1. In Section 17 we use Linnik's theorem from analytic number theory in order to find auxiliary numbers in our main algorithm, and our main algorithm is presented in Section 18.

For the purposes of this paper, commutative rings have an identity element 1, which may be 0. If R is a commutative ring, let R^* denote the group of elements of R that have a multiplicative inverse in R.

2. Integral lattices

We begin with some background on lattices and on lattice automorphisms (see also [6]).

Definition 2.1. A **lattice** or **integral lattice** is a finitely generated abelian group L with a map $\langle \cdot, \cdot \rangle : L \times L \to \mathbb{Z}$ that is

- bilinear: $\langle x, y+z \rangle = \langle x, y \rangle + \langle x, z \rangle$ and $\langle x+y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ for all $x, y, z \in L$,
- symmetric: $\langle x, y \rangle = \langle y, x \rangle$ for all $x, y \in L$, and
- positive definite: $\langle x, x \rangle > 0$ if $0 \neq x \in L$.

As a group, L is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$, which is called the **rank** of L and is denoted $\operatorname{rank}(L)$. In algorithms, a lattice is specified by a Gram matrix $(\langle b_i, b_j \rangle)_{i,j=1}^n$ associated to a $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$ and an element of a lattice is specified by its coefficient vector on the same basis. The inner product $\langle \cdot, \cdot \rangle$ extends to a real-valued inner product on $L \otimes_{\mathbb{Z}} \mathbb{R}$ and makes $L \otimes_{\mathbb{Z}} \mathbb{R}$ into a Euclidean vector space.

Definition 2.2. The **standard lattice** of rank n is $\mathbb{Z}^n$ with $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$. Its Gram matrix is the $n \times n$ identity matrix.

Definition 2.3. The determinant $\det(L)$ of a lattice L is the determinant of the Gram matrix of L; equivalently, $\det(L)$ is the order of the cokernel of the map $L \to \operatorname{Hom}(L, \mathbb{Z})$, $x \mapsto (y \mapsto \langle x, y \rangle)$. A lattice L is **unimodular** if this map is bijective, i.e., if $\det(L) = 1$.

Definition 2.4. An **isomorphism** $L \xrightarrow{\sim} M$ of lattices is a group isomorphism φ from L to M that respects the lattice structures, i.e., $\langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$ for all $x, y \in L$. If such a map φ exists, then L and M are **isomorphic** lattices. An **automorphism** of a lattice L is an isomorphism from L to itself. The set of automorphisms of L is a finite group $\operatorname{Aut}(L)$ whose center contains -1.

In algorithms, isomorphisms are specified by their matrices on the given bases of L and M.

Examples 2.5.

(i) "Random" lattices have $\operatorname{Aut}(L) = \{\pm 1\}$.

(ii) Letting S_n denote the symmetric group on n letters and $\rtimes$ denote semidirect product, we have $\operatorname{Aut}(\mathbb{Z}^n) \cong \{\pm 1\}^n \rtimes S_n$. (The standard basis vectors can be permuted, and signs changed.)

(iii) If L is the equilateral triangular lattice in the plane, then $\operatorname{Aut}(L)$ is the symmetry group of the regular hexagon, which is a dihedral group of order 12.

3. Reduced bases and automorphisms

The main result of this section is Proposition 3.4, in which we obtain some bounds for LLL-reduced bases of unimodular lattices. We will use this result to give bounds on

the complexity of our algorithms and to show that the Witt-Picard group (Definition 14.1 below) is finite. If L is a lattice and $a \in L \otimes_{\mathbb{Z}} \mathbb{R}$, let $|a| = \langle a, a\rangle^{1/2}$.

Definition 3.1. If $\{b_1, \ldots, b_n\}$ is a basis for a lattice L, and $\{b_1^*, \ldots, b_n^*\}$ is its Gram-Schmidt orthogonalization, and $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*$ with $\mu_{ij} \in \mathbb{R}$, then $\{b_1, \ldots, b_n\}$ is **LLL-reduced** if

(i) $|\mu_{ij}| \leq \frac{1}{2}$ for all $j < i \leq n$, and
(ii) $|b_i^*|^2 \leq 2|b_{i+1}^*|^2$ for all $i < n$.

Remark 3.2. The LLL basis reduction algorithm [5] takes as input a lattice, and produces an LLL-reduced basis of the lattice, in polynomial time.

Lemma 3.3. *If $a = (\mu_{ij})_{ij} \in \mathrm{M}(n, \mathbb{R})$ is a lower-triangular real matrix with $\mu_{ii} = 1$ for all i and $|\mu_{ij}| \leq 1/2$ for all $j < i$, and $a^{-1} = (\nu_{ij})_{ij}$, then*

$$|\nu_{ij}| \leq \begin{cases} 0 & \text{if } i < j \\ 1 & \text{if } i = j \\ \frac{1}{3}\left(\frac{3}{2}\right)^{i-j} & \text{if } i > j. \end{cases}$$

Proof. Define $e \in \mathrm{M}(n, \mathbb{R})$ by $e_{ij} = 0$ if $j \geq i$ and $e_{ij} = \frac{1}{2}$ if $j < i$. Define $h \in \mathrm{M}(n, \mathbb{R})$ by $h_{i+1,i} = 1$ for $i = 1, \ldots, n-1$ and $h_{ij} = 0$ otherwise. Then $e = \sum_{j=1}^{\infty} \frac{1}{2} h^j = \frac{h}{2(1-h)}$. Thus, $1 - e = (1 - 3h/2)/(1 - h)$ and

$$(1-e)^{-1} = (1-h)/(1-3h/2)$$
$$= (1-h)\sum_{j=0}^{\infty}\left(\frac{3}{2}\right)^j h^j = \sum_{j=0}^{\infty}\left(\frac{3}{2}\right)^j h^j - \sum_{j=0}^{\infty}\left(\frac{3}{2}\right)^j h^{j+1} =$$
$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ \frac{3}{2} & 1 & \cdots & 0 \\ (\frac{3}{2})^2 & \frac{3}{2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ (\frac{3}{2})^{n-1} & (\frac{3}{2})^{n-2} & \cdots & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ \frac{3}{2} & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ (\frac{3}{2})^{n-2} & (\frac{3}{2})^{n-3} & \cdots & \frac{3}{2} & 1 & 0 \end{pmatrix},$$

which has ij entry 0 if $i < j$, and 1 if $i = j$, and $\frac{1}{3}\left(\frac{3}{2}\right)^{i-j}$ if $i > j$.

Since $e^n = 0 = (1-a)^n$, we have $(1-e)^{-1} = \sum_{i=0}^{n-1} e^i$ and $a^{-1} = \sum_{i=0}^{n-1}(1-a)^i$. If $c = (c_{ij})_{ij} \in \mathrm{M}(n, \mathbb{R})$, let $|c|$ denote $(|c_{ij}|)_{ij}$. If $c, d \in \mathrm{M}(n, \mathbb{R})$, then $c \leq d$ means that $c_{ij} \leq d_{ij}$ for all i and j. We have $|a^{-1}| \leq \sum_{i=0}^{n-1} |1-a|^i \leq \sum_{i=0}^{n-1} e^i = (1-e)^{-1}$. This gives the desired result. □

Proposition 3.4. *If $\{b_1, \ldots, b_n\}$ is an LLL-reduced basis for an integral unimodular lattice L and $\{b_1^*, \ldots, b_n^*\}$ is its Gram-Schmidt orthogonalization, then*

(i) $2^{1-i} \leq |b_i^*|^2 \leq 2^{n-i}$,
(ii) $|b_i|^2 \leq 2^{n-1}$ *for all* $i \in \{1, \ldots, n\}$,
(iii) $|\langle b_i, b_j\rangle| \leq 2^{n-1}$ *for all* i *and* j,

(iv) *if* $\sigma \in \mathrm{Aut}(L)$, *and for each* i *we have* $\sigma(b_i) = \sum_{j=1}^n a_{ij} b_j$ *with* $a_{ij} \in \mathbb{Z}$, *then* $|a_{ij}| \le 3^{n-1}$ *for all* i *and* j.

Proof. It follows from Definition 3.1 that for all $1 \le j \le i \le n$ we have $|b_i^*|^2 \le 2^{j-i}|b_j^*|^2$, so for all i we have

$$2^{1-i}|b_1^*|^2 \le |b_i^*|^2 \le 2^{n-i}|b_n^*|^2.$$

Since L is integral we have $|b_1^*|^2 = |b_1|^2 = \langle b_1, b_1\rangle \ge 1$, so $|b_i^*|^2 \ge 2^{1-i}$. Letting $L_i = \sum_{j=1}^i \mathbb{Z} b_j$, we have $|b_i^*| = \det(L_i)/\det(L_{i-1})$. Since L is integral and unimodular, $|b_n^*| = \det(L_n)/\det(L_{n-1}) = 1/\det(L_{n-1}) \le 1$, so $|b_i^*| \le 2^{n-i}$, giving (i).

Since $\{b_i^*\}$ is orthogonal we have

$$\begin{aligned}|b_i|^2 = |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2 &\le 2^{n-i} + \frac{1}{4}\sum_{j=1}^{i-1} 2^{n-j} \\ &= 2^{n-i} + (2^{n-2} - 2^{n-i-1}) = 2^{n-2} + 2^{n-i-1} \le 2^{n-1},\end{aligned}$$

giving (ii). Now (iii) follows by applying the Cauchy-Schwarz inequality $|\langle b_i, b_j\rangle| \le |b_i||b_j|$ and (ii).

For (iv), define $\{c_1, \dots, c_n\}$ to be the basis of L that is dual to $\{b_1, \dots, b_n\}$, i.e., $\langle c_i, b_j\rangle = \delta_{ij}$ for all i and j, where δ_{ij} is the Kronecker delta symbol. Then $a_{ij} = \langle c_j, \sigma(b_i)\rangle$ so

$$|a_{ij}| \le |c_j||\sigma(b_i)| = |c_j||b_i|. \tag{3.5}$$

Define $\mu_{ii} = 1$ for all i and $\mu_{ij} = 0$ if $i < j$, and let $M = (\mu_{ij})_{ij} \in \mathrm{M}(n, \mathbb{R})$. Then $(b_1\ b_2\ \cdots\ b_n) = (b_1^*\ b_2^*\ \cdots\ b_n^*)M^t$. For $0 \ne x \in L \otimes_{\mathbb{Z}} \mathbb{R}$, define $x^{-1} = x/\langle x, x\rangle$. This inverse map is characterized by the properties that $\langle x, x^{-1}\rangle = 1$ and $\mathbb{R}x^{-1} = \mathbb{R}x$; so $(x^{-1})^{-1} = x$. Since the basis dual to $\{b_i^*\}_i$ is $\{(b_i^*)^{-1}\}_i$, and M gives the change of basis from $\{b_i^*\}_i$ to $\{b_i\}_i$, it follows that the matrix $(M^t)^{-1}$ gives the change of basis from $\{(b_i^*)^{-1}\}_i$ to $\{c_i\}_i$. Thus,

$$(c_1\ \cdots\ c_n) = ((b_1^*)^{-1}\ \cdots\ (b_n^*)^{-1})M^{-1}.$$

Letting $(\nu_{ij})_{ij} = M^{-1}$, by Lemma 3.3 we have $c_j = \sum_{i \ge j} (b_i^*)^{-1}\nu_{ij}$ with $\nu_{ii} = 1$ and $|\nu_{ij}| \le \frac{1}{3}\left(\frac{3}{2}\right)^{i-j}$ if $i > j$. By (i) we have $|(b_i^*)^{-1}|^2 \le 2^{i-1}$. Thus,

$$\begin{aligned}|c_j|^2 \le \sum_{i \ge j} 2^{i-1}\nu_{ij}^2 &\le 2^{j-1} + \frac{1}{9}\sum_{i>j} 2^{i-1}\left(\frac{9}{4}\right)^{i-j} \le 2^{j-1} + \frac{2^{j-1}}{9}\sum_{k=1}^{n-j}\left(\frac{9}{2}\right)^k \\ &= 2^{j-1} + \frac{2^j}{63}\left[\left(\frac{9}{2}\right)^{n-j+1} - \frac{9}{2}\right] = \frac{2^{j-1}}{7}\left[\left(\frac{9}{2}\right)^{n-j} + 6\right] \\ &\le \frac{1}{7}\left(\frac{9}{2}\right)^{n-1} + \frac{6}{7}\left(\frac{9}{2}\right)^{n-1} = \left(\frac{9}{2}\right)^{n-1}.\end{aligned}$$

Now by (ii) and (3.5) we have $|a_{ij}|^2 \le 9^{n-1}$, as desired. □

Remark 3.6. It is easier to get the weaker bound $|a_{ij}| \leq 2^{\binom{n}{2}}$, as follows. Write $b_j = b_j^{\#} + y$ with $y \in \sum_{i \neq j} \mathbb{R} b_i$ and $b_j^{\#}$ orthogonal to $\sum_{i \neq j} \mathbb{R} b_i$. With c_j as in the proof of Proposition 3.4, we have $c_j = (b_j^{\#})^{-1}$, by the characterizations of $(b_j^{\#})^{-1}$ and c_j. Since $1 = \det(L) = \det(\sum_{i \neq j} \mathbb{Z} b_i)|b_j^{\#}|$ we have

$$|c_j| = |\det(\sum_{i \neq j} \mathbb{Z} b_i)| \leq \prod_{i \neq j} |b_i| \leq 2^{(n-1)^2/2}$$

by Hadamard's inequality and Proposition 3.4(ii). By (3.5) and Proposition 3.4(ii) we have $|a_{ij}| \leq 2^{\binom{n}{2}}$.

4. Short vectors in lattice cosets

We show how to find the unique vector of length 1 in a suitable lattice coset, when such a vector exists.

Proposition 4.1. *Suppose L is an integral lattice, $3 \leq m \in \mathbb{Z}$, and $C \in L/mL$. Then the coset C contains at most one element $x \in L$ with $\langle x, x \rangle = 1$.*

Proof. Suppose $x, y \in C$, with $\langle x, x \rangle = \langle y, y \rangle = 1$. Since $x, y \in C$, there exists $w \in L$ such that $x - y = mw$. Using the triangle inequality, we have

$$m\langle w, w \rangle^{1/2} = \langle x - y, x - y \rangle^{1/2} \leq \langle x, x \rangle^{1/2} + \langle y, y \rangle^{1/2} = 1 + 1 = 2.$$

Since $m \geq 3$ and $\langle w, w \rangle \in \mathbb{Z}_{\geq 0}$, we have $w = 0$, and thus $y = x$. □

Algorithm 4.2. Given a rank n integral lattice L, an integer m such that $m \geq 2^{n/2} + 1$, and $C \in L/mL$, the algorithm computes all $y \in C$ with $\langle y, y \rangle = 1$.

(i) Compute an LLL-reduced basis for mL and use it as in §10 of [6] to compute $y \in C$ such that $\langle y, y \rangle \leq (2^n - 1)\langle x, x \rangle$ for all $x \in C$, i.e., to find an approximate solution to the nearest vector problem.
(ii) Compute $\langle y, y \rangle$.
(iii) If $\langle y, y \rangle = 1$, output y.
(iv) If $\langle y, y \rangle \neq 1$, output "there is no $y \in C$ with $\langle y, y \rangle = 1$".

Proposition 4.3. *Algorithm 4.2 is a deterministic polynomial-time algorithm that, given a integral lattice L, an integer m such that $m \geq 2^{n/2} + 1$ where $n = \operatorname{rank}(L)$, and $C \in L/mL$, outputs all $y \in C$ with $\langle y, y \rangle = 1$. The number of such y is 0 or 1.*

Proof. Suppose $x \in C$ with $\langle x, x \rangle = 1$. Since $x, y \in C$, there exists $w \in L$ such that $x - y = mw$. Using the triangle inequality, we have

$$m\langle w, w \rangle^{1/2} = \langle x - y, x - y \rangle^{1/2} \leq \langle x, x \rangle^{1/2} + \langle y, y \rangle^{1/2} < (1 + 2^{n/2})\langle x, x \rangle^{1/2} \leq m,$$

so $\langle w, w \rangle^{1/2} < 1$. Since $\langle w, w \rangle \in \mathbb{Z}_{\geq 0}$, we have $w = 0$, and thus $y = x$. If $\langle y, y \rangle \neq 1$, there is no $x \in C$ with $\langle x, x \rangle = 1$. □

5. G-lattices

We introduce G-lattices and G-isomorphisms. From now on, suppose that G is a finite abelian group equipped with a fixed element u of order 2, and that $n = \#G/2 \in \mathbb{Z}$.

Definition 5.1. Let S be a set of coset representatives of $G/\langle u \rangle$ (i.e., $\#S = n$ and $G = S \sqcup uS$), and for simplicity take S so that $1 \in S$.

Definition 5.2. A **G-lattice** is a lattice L together with a group homomorphism $f : G \to \mathrm{Aut}(L)$ such that $f(u) = -1$. For each $\sigma \in G$ and $x \in L$, define $\sigma x \in L$ by $\sigma x = f(\sigma)(x)$.

The abelian group G is specified by a multiplication table. The G-lattice L is specified as a lattice along with, for each $\sigma \in G$, the matrix describing the action of σ on L.

Definition 5.3. If L and M are G-lattices, then a **G-isomorphism** is an isomorphism $\varphi : L \xrightarrow{\sim} M$ of lattices that respects the G-actions, i.e., $\varphi(\sigma x) = \sigma\varphi(x)$ for all $x \in L$ and $\sigma \in G$. If such an isomorphism exists, we say that L and M are **G-isomorphic**, or isomorphic as G-lattices.

6. The modified group ring $\mathbb{Z}\langle G \rangle$

We define a modified group ring $A\langle G \rangle$ whenever A is a commutative ring. We will usually take $A = \mathbb{Z}$, but will also take $A = \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Q}$ and $\mathbb{C}$.

If H is a group and A is a commutative ring, the group ring $A[H]$ is the set of formal sums $\sum_{\sigma \in H} a_\sigma \sigma$ with $a_\sigma \in A$, with addition defined by

$$\sum_{\sigma \in H} a_\sigma \sigma + \sum_{\sigma \in H} b_\sigma \sigma = \sum_{\sigma \in H} (a_\sigma + b_\sigma)\sigma$$

and multiplication defined by

$$(\sum_{\sigma \in H} a_\sigma \sigma)(\sum_{\tau \in H} b_\tau \tau) = \sum_{\rho \in H} (\sum_{\sigma\tau = \rho} a_\sigma b_\tau)\rho.$$

For example, if H is a cyclic group of order m and h is a generator, then as rings we have $\mathbb{Z}[X]/(X^m - 1) \cong \mathbb{Z}[H]$ via the map $\sum_{i=0}^{m-1} a_i X^i \mapsto \sum_{i=0}^{m-1} a_i h^i$.

Definition 6.1. If A is a commutative ring, then writing 1 for the identity element of the group G, we define the **modified group ring**

$$A\langle G \rangle = A[G]/(u + 1).$$

Every G-lattice L is a $\mathbb{Z}\langle G \rangle$-module, where one uses the G-action on L to define ax whenever $x \in L$ and $a \in \mathbb{Z}\langle G \rangle$. This is why we consider $A\langle G \rangle$ rather than the standard group ring $A[G]$. Considering groups equipped with an element of order 2 allows us to include the cyclotomic rings $\mathbb{Z}[X]/(X^{2^k} + 1)$ in our theory.

Definition 6.2. Define the **scaled trace function** $t : A\langle G\rangle \to A$ by

$$t(\sum_{\sigma\in G} a_\sigma\sigma) = a_1 - a_u.$$

This is well defined since the restriction of t to $(u+1)A[G]$ is 0. The map t is the A-linear map satisfying $t(1) = 1$, $t(u) = -1$, and $t(\sigma) = 0$ if $\sigma \in G$ and $\sigma \neq 1, u$.

Definition 6.3. For $a = \sum_{\sigma\in G} a_\sigma\sigma \in A\langle G\rangle$, define $\overline{a} = \sum_{\sigma\in G} a_\sigma\sigma^{-1}$.

The map $a \mapsto \overline{a}$ is a ring automorphism of $A\langle G\rangle$. Since $\overline{\overline{a}} = a$, it is an involution. (An involution is a ring automorphism that is its own inverse.) One can think of this map as mimicking complex conjugation (cf. Lemma 7.3(i)).

Remark 6.4. If L is a G-lattice and $x, y \in L$, then $\langle \sigma x, \sigma y\rangle = \langle x, y\rangle$ for all $\sigma \in G$ by Definition 2.4. It follows that $\langle ax, y\rangle = \langle x, \overline{a}y\rangle$ for all $a \in \mathbb{Z}\langle G\rangle$. This "hermitian" property of the inner product is the main reason for introducing the involution.

Definition 6.5. For $x, y \in \mathbb{Z}\langle G\rangle$ define $\langle x, y\rangle_{\mathbb{Z}\langle G\rangle} = t(x\overline{y})$.

Recall that $n = \#G/2$ and S is a set of coset representatives of $G/\langle u\rangle$. The following two results are straightforward.

Lemma 6.6. *Suppose A is a commutative ring. Then:*

(i) $A\langle G\rangle = \{\sum_{\sigma\in S} a_\sigma\sigma : a_\sigma \in A\} = \bigoplus_{\sigma\in S} A\sigma$;
(ii) *if $a = \sum_{\sigma\in S} a_\sigma\sigma \in A\langle G\rangle$, then*
  (a) $t(a) = a_1$,
  (b) $t(\bar{a}) = t(a)$,
  (c) $t(a\bar{a}) = \sum_{\sigma\in S} a_\sigma^2$,
  (d) $a = \sum_{\sigma\in S} t(\sigma^{-1}a)\sigma$,
  (e) *if $t(ab) = 0$ for all $b \in A\langle G\rangle$, then $a = 0$.*

Proposition 6.7. (i) *The additive group of the ring $\mathbb{Z}\langle G\rangle$ is a G-lattice of rank n, with lattice structure defined by $\langle\,\cdot\,,\,\cdot\,\rangle_{\mathbb{Z}\langle G\rangle}$ and G-action defined by $\sigma x = \sigma x$ where the right hand side is ring multiplication in $\mathbb{Z}\langle G\rangle$.*
(ii) *As lattices, we have $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}^n$.*

Definition 6.8. We call $\mathbb{Z}\langle G\rangle$ the **standard G-lattice**.

The set S of coset representatives for $G/\langle u\rangle$ is an orthonormal basis for the standard G-lattice.

Example 6.9. Suppose $G = H \times \langle u\rangle$ with $H \cong \mathbb{Z}/n\mathbb{Z}$. Then $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[H] \cong \mathbb{Z}[X]/(X^n - 1)$ as rings and as lattices. When n is odd (so G is cyclic), then, sending X to $-X$, we have $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[X]/(X^n - 1) \cong \mathbb{Z}[X]/(X^n + 1)$.

Example 6.10. If G is cyclic, then $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[X]/(X^n + 1)$, identifying X with a generator of G. If G is cyclic of order 2^r, then $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[X]/(X^{2^{r-1}} + 1) \cong \mathbb{Z}[\zeta_{2^r}]$, where ζ_{2^r} is a primitive 2^r-th root of unity.

Remark 6.11. The ring $\mathbb{Z}\langle G\rangle$ is an integral domain if and only if G is cyclic and n is a power of 2 (including $2^0 = 1$). (If $g \in G$ is an element whose order is odd or 2, and $g \notin \{1, u\}$, then $g - 1$ is a zero divisor.)

7. The modified group ring over fields

The main result of this section is Lemma 7.3, which we will use repeatedly in the rest of the paper. Recall that G is a finite abelian group of order $2n$ equipped with an element u of order 2. If R is a commutative ring, then a commutative R-algebra is a commutative ring A equipped with a ring homomorphism from R to A.

If K is a subfield of $\mathbb{C}$ and E is a commutative K-algebra with $\dim_K(E) < \infty$, let Φ_E denote the set of K-algebra homomorphisms from E to $\mathbb{C}$. Then $\mathbb{C}^{\Phi_E}$ is a $\mathbb{C}$-algebra with coordinate-wise operations. The next result is not only useful for studying modified group rings, but also comes in handy in Proposition 15.2 below.

Lemma 7.1. *Suppose K is a subfield of $\mathbb{C}$ and E is a commutative K-algebra with $\dim_K(E) < \infty$. Assume $\#\Phi_E = \dim_K(E)$. Then:*

(i) *identifying Φ_E with $\{\mathbb{C}$-algebra homomorphisms $E_{\mathbb{C}} = \mathbb{C} \otimes_K E \to \mathbb{C}\}$, the map $E_{\mathbb{C}} \to \mathbb{C}^{\Phi_E}$, $x \mapsto (\varphi(x))_{\varphi\in\Phi_E}$ is an isomorphism of $\mathbb{C}$-algebras;*

(ii) *$\bigcap_{\varphi\in\Phi_E} \ker(\varphi) = 0$ in E;*

(iii) *there is a finite collection $\{K_j\}_{j=1}^d$ of finite extension fields of K such that $E \cong K_1 \times \cdots \times K_d$ as K-algebras.*

Proof. By the Corollaire to Proposition 1 in V.6.3 of [1], the set Φ_E is a $\mathbb{C}$-basis for $\mathrm{Hom}_K(E, \mathbb{C}) = \mathrm{Hom}_{\mathbb{C}}(E_{\mathbb{C}}, \mathbb{C})$, so the $\mathbb{C}$-algebra homomorphism in (i) is an isomorphism. Part (ii) follows immediately from (i).

By Proposition 2 in V.6.3 of [1], the K-algebra E is what Bourbaki calls an étale K-algebra, and (iii) then follows from Theorem 4 in V.6.7 of [1]. □

Definition 7.2. Let Ψ denote the set of ring homomorphisms from $\mathbb{Q}\langle G\rangle$ to $\mathbb{C}$. We identify Ψ with the set of K-algebra homomorphisms from $K\langle G\rangle$ to $\mathbb{C}$, where K is any subfield of $\mathbb{C}$. The set Ψ can also be identified with the set of group homomorphisms $\psi : G \to \mathbb{C}^*$ such that $\psi(u) = -1$.

We have $\#\Psi = n$, since $\#\mathrm{Hom}(G, \mathbb{C}^*) = \#G = 2n$ and the restriction map $\mathrm{Hom}(G, \mathbb{C}^*) \to \mathrm{Hom}(\langle u\rangle, \mathbb{C}^*)$ is surjective. This allows us to apply Lemma 7.1 with $E = K\langle G\rangle$. If $a \in \mathbb{C}\langle G\rangle$, then a acts on the $\mathbb{C}$-vector space $\mathbb{C}\langle G\rangle$ by multiplication, and for $\psi \in \Psi$ the $\psi(a)$ are the eigenvalues for this linear transformation. Lemma 7.3(ii) justifies thinking of the map t of Definition 6.2 as a scaled trace function.

Lemma 7.3. (i) *If $\psi \in \Psi$, then $\overline{\psi(\alpha)} = \psi(\bar{\alpha})$ for all $\alpha \in \mathbb{R}\langle G\rangle$.*

(ii) *If $a \in \mathbb{C}\langle G\rangle$, then $t(a) = \frac{1}{n}\sum_{\psi\in\Psi} \psi(a)$.*

(iii) *If K is a subfield of $\mathbb{C}$, then $\bigcap_{\psi\in\Psi} \ker(\psi) = 0$ in $K\langle G\rangle$.*

(iv) *The map $\mathbb{C}\langle G\rangle \to \mathbb{C}^\Psi$, $x \mapsto (\psi(x))_{\psi\in\Psi}$ is an isomorphism of $\mathbb{C}$-algebras.*

(v) *There are number fields* $K_1, \ldots, K_d$ *such that* $\mathbb{Q}\langle G\rangle \cong K_1 \times \cdots \times K_d$ *as* $\mathbb{Q}$*-algebras.*

(vi) *Suppose* K *is a subfield of* $\mathbb{C}$ *and* $\alpha \in K\langle G\rangle$*. Then* $\alpha \in K\langle G\rangle^*$ *if and only if* $\psi(\alpha) \neq 0$ *for all* $\psi \in \Psi$*.*

(vii) *If* $z \in \mathbb{R}\langle G\rangle$ *is such that* $\psi(z) \in \mathbb{R}$ *for all* $\psi \in \Psi$ *and* $\sum_{\in} (x\overline{x}z) \geq 0$ *for all* $x \in \mathbb{R}\langle G\rangle$*, then* $\psi(z) \geq 0$ *for all* $\psi \in \Psi$*.*

Proof. For (i), since G is finite, $\psi(\sigma)$ is a root of unity for all $\sigma \in G$. Thus, $\overline{\psi(\sigma)} = \psi(\sigma)^{-1} = \psi(\sigma^{-1}) = \psi(\bar{\sigma})$. The $\mathbb{R}$-linearity of ψ and of $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ now imply (i).

We have $\frac{1}{n}\sum_{\psi\in\Psi} \psi(1) = 1 = t(1)$, and $\frac{1}{n}\sum_{\in} \psi(u) = -1 = t(u)$, and for each $\sigma \notin \langle u\rangle$ we have

$$\sum_{\in} \psi(\sigma) = -\sum_{\substack{\in \mathrm{Hom}(G,\mathbb{C}^*)\\ \psi(u)=1}} \psi(\sigma) = -\sum_{\in \mathrm{Hom}(G/\langle u\rangle,\mathbb{C}^*)} \psi(\sigma \bmod \langle u\rangle) = 0 = nt(\sigma).$$

Extending $\mathbb{C}$-linearly gives (ii).

If K is a subfield of $\mathbb{C}$, then $\Psi = n = \dim_K K\langle G\rangle$. Thus we can apply Lemma 7.1, giving (iii), (iv), and (v).

By (iv) we have $\mathbb{C}\langle G\rangle^* \xrightarrow{\sim} (\mathbb{C}^*)^\Psi$. This gives (vi) when $K = \mathbb{C}$. If K is a subfield of $\mathbb{C}$ and $x \in K\langle G\rangle \cap \mathbb{C}\langle G\rangle^*$ then multiplication by x is an injective map from $K\langle G\rangle$ to itself, so is also surjective, so $x \in K\langle G\rangle^*$. Thus $K\langle G\rangle^* = K\langle G\rangle \cap \mathbb{C}\langle G\rangle^*$, and (vi) follows.

For (vii), applying Lemma 7.1(iii) with $K = \mathbb{R}$ gives an $\mathbb{R}$-algebra isomorphism $\mathbb{R}\langle G\rangle \xrightarrow{\sim} \mathbb{R}^r \times \mathbb{C}^s$. The set $\Psi = \{\psi_j\}_{j=1}^{r+2s}$ consists of the r projection maps $\psi_j : \mathbb{R}\langle G\rangle \to \mathbb{R} \subset \mathbb{C}$ for $1 < j \leq r$, along with the s projection maps $\psi_j : \mathbb{R}\langle G\rangle \to \mathbb{C}$ and their complex conjugates $\psi_{s+j} = \overline{\psi_j}$ for $r+1 \leq j \leq r+s$. By (i), if $x = (x_1, \ldots, x_r, y_1, \ldots, y_s) \in \mathbb{R}^r \times \mathbb{C}^s$, then $\overline{x} = (x_1, \ldots, x_r, \overline{y_1}, \ldots, \overline{y_s})$. Taking x to have 1 in the j-th position and 0 everywhere else, we have $0 \leq \sum_{\in} \psi(x\overline{x}z) = \psi_j(z)$ if $1 \leq j \leq r$ and $2\psi_j(z)$ otherwise, giving (vii). □

8. Ideal lattices

As before, G is a finite abelian group of order $2n$ equipped with an element u of order 2. Theorem 8.2 below gives a way to view certain ideals I in $\mathbb{Z}\langle G\rangle$ as G-lattices, and Theorem 8.5 characterizes the ones that are G-isomorphic to $\mathbb{Z}\langle G\rangle$.

Definition 8.1. A *fractional* $\mathbb{Z}\langle G\rangle$*-ideal* is a finitely generated $\mathbb{Z}\langle G\rangle$-module in $\mathbb{Q}\langle G\rangle$ that spans $\mathbb{Q}\langle G\rangle$ over $\mathbb{Q}$. An *invertible* fractional $\mathbb{Z}\langle G\rangle$-ideal is a fractional $\mathbb{Z}\langle G\rangle$-ideal I such that there is a fractional $\mathbb{Z}\langle G\rangle$-ideal J with $IJ = \mathbb{Z}\langle G\rangle$, where IJ is the fractional $\mathbb{Z}\langle G\rangle$-ideal generated by the products of elements from I and J.

Theorem 8.2. *Suppose* $I \subset \mathbb{Q}\langle G\rangle$ *is a fractional* $\mathbb{Z}\langle G\rangle$*-ideal and* $w \in \mathbb{Q}\langle G\rangle$*. Suppose that* $I\overline{I} \subset \mathbb{Z}\langle G\rangle \cdot w$ *and* $\psi(w) \in \mathbb{R}_{>0}$ *for all* $\psi \in \Psi$*. Then:*

(i) $\overline{w} = w$*;*

(ii) $w \in \mathbb{Q}\langle G\rangle^*$*;*

(iii) *I is a G-lattice, with G-action defined by multiplication in $\mathbb{Z}\langle G\rangle$, and with lattice structure defined by $\langle x, y\rangle_{I,w} = t(x\overline{y}/w)$, with t as in Definition 6.2.*

Proof. By Lemma 7.3(i) we have $\psi(w) = \overline{\psi(w)} = \psi(\bar{w})$ for all $\psi \in \Psi$. Now (i) follows from Lemma 7.3(iii). Lemma 7.3(vi) implies (ii). Note that $\frac{x\overline{y}}{w} \in \mathbb{Z}\langle G\rangle$, since w generates the ideal $I\overline{I}$. Part (iii) now follows from (i) and (ii) of Lemma 7.3. □

Definition 8.3. Let $L_{(I,w)}$ denote the G-lattice I in Theorem 8.2(iii).

Example 8.4. We have $L_{(\mathbb{Z}\langle G\rangle,1)} = \mathbb{Z}\langle G\rangle$.

Theorem 8.5. *Suppose that I_1 and I_2 are fractional $\mathbb{Z}\langle G\rangle$-ideals, that $w_1, w_2 \in \mathbb{Q}\langle G\rangle$, that $I_1\overline{I_1} \subset \mathbb{Z}\langle G\rangle \cdot w_1$ and $I_2\overline{I_2} \subset \mathbb{Z}\langle G\rangle \cdot w_2$, and that $\psi(w_1), \psi(w_2) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$. Let $L_j = L_{(I_j,w_j)}$ for $j = 1, 2$. Then sending v to multiplication by v gives a bijection from*

$$\{v \in \mathbb{Q}\langle G\rangle : I_1 = vI_2, w_1 = v\overline{v}w_2\} \quad to \quad \{G\text{-isomorphisms } L_2 \xrightarrow{\sim} L_1\}$$

and gives a bijection from

$$\{v \in \mathbb{Q}\langle G\rangle : I_1 = v\mathbb{Z}\langle G\rangle, w_1 = v\overline{v}\} \quad to \quad \{G\text{-isomorphisms } \mathbb{Z}\langle G\rangle \xrightarrow{\sim} L_1\}.$$

In particular, L_1 is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if there exists $v \in \mathbb{Q}\langle G\rangle$ such that $I_1 = (v)$ and $w_1 = v\overline{v}$.

Proof. Any $\mathbb{Z}\langle G\rangle$-module isomorphism $\varphi : L_2 \xrightarrow{\sim} L_1$ extends to a $\mathbb{Q}\langle G\rangle$-module isomorphism from $L_2 \otimes \mathbb{Q} = \mathbb{Q}\langle G\rangle$ to $L_1 \otimes \mathbb{Q} = \mathbb{Q}\langle G\rangle$, and any such map is multiplication by some $v \in \mathbb{Q}\langle G\rangle^*$. Conversely, for $v \in \mathbb{Q}\langle G\rangle$, multiplication by v defines a $\mathbb{Z}\langle G\rangle$-module isomorphism from L_2 to L_1 if and only if $I_1 = vI_2$. When $I_1 = vI_2$, multiplication by v is a G-isomorphism from L_2 to L_1 if and only if $w_1 = v\overline{v}w_2$; this follows from Lemma 6.6(ii)(e), since for all $a, b \in I_2$ we have $\langle a, b\rangle_{I_2,w_2} = t\left(\frac{a\bar{b}}{w_2}\right)$ and $\langle av, bv\rangle_{I_1,w_1} = t\left(\frac{a\bar{b}v\overline{v}}{w_1}\right)$. This gives the first desired bijection. Taking $I_2 = \mathbb{Z}\langle G\rangle$ and $w_2 = 1$ gives the second bijection. □

We next show how to recover the Gentry-Szydlo algorithm from Theorem 1.1. The goal of the Gentry-Szydlo algorithm is to find a generator v of a principal ideal I of finite index in the ring $R = \mathbb{Z}[X]/(X^n - 1)$, given $v\overline{v}$ and a $\mathbb{Z}$-basis for I. Here, n is an odd prime, and for $v = v(X) = \sum_{i=0}^{n-1} a_i X^i \in R$, its "reversal" is $\overline{v} = v(X^{-1}) = a_0 + \sum_{i=1}^{n-1} a_{n-i} X^i \in R$. We take G to be a cyclic group of order $2n$. Then $R \cong \mathbb{Z}\langle G\rangle$ as in Example 6.9, and we identify R with $\mathbb{Z}\langle G\rangle$. Let $w = v\overline{v} \in \mathbb{Z}\langle G\rangle$ and let $L = L_{(I,w)}$ as in Definition 8.3. Then L is the "implicit orthogonal lattice" in §7.2 of [3]. Once one knows w and a $\mathbb{Z}$-basis for I, then one knows L. Theorem 1.1 produces a G-isomorphism $\varphi : \mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ in polynomial time, and thus (as in Theorem 8.5) gives a generator $v = \varphi(1)$ in polynomial time.

9. Invertible G-lattices

Recall that G is a finite abelian group of order $2n$, with a fixed element u of order 2, and S is a set of coset representatives for $G/\langle u\rangle$. In Definition 9.5 we introduce the concept of an invertible G-lattice. The inverse of such a lattice L is the G-lattice $\overline{L}$ given in Definition 9.1.

Definition 9.1. If L is a G-lattice, then the G-lattice $\overline{L}$ is a lattice equipped with a lattice isomorphism $L \xrightarrow{\sim} \overline{L}$, $x \mapsto \overline{x}$ and a group homomorphism $G \to \mathrm{Aut}(\overline{L})$ defined by $\sigma\overline{x} = \overline{\sigma^{-1}x}$ for all $\sigma \in G$ and $x \in L$, i.e., $\overline{\sigma x} = \overline{\sigma}\,\overline{x}$.

Existence follows by taking $\overline{L}$ to be L with the appropriate G-action. The G-lattice $\overline{L}$ is unique up to G-isomorphism, and we have $\overline{\overline{L}} = L$.

Definition 9.2. If L is a G-lattice, define the **lifted inner product**

$$\cdot : L \times \overline{L} \to \mathbb{Z}\langle G\rangle \quad \text{by} \quad x \cdot \overline{y} = \sum_{\sigma\in S} \langle x, \sigma y\rangle \sigma \in \mathbb{Z}\langle G\rangle.$$

This lifted inner product is independent of the choice of the set S, and is $\mathbb{Z}\langle G\rangle$-bilinear, i.e., $(ax)\cdot\overline{y} = x\cdot(a\overline{y}) = a(x\cdot\overline{y})$ for all $a \in \mathbb{Z}\langle G\rangle$ and all $x, y \in L$. We have

$$\langle x, y\rangle = t(x \cdot \overline{y}) \tag{9.3}$$

and $x \cdot \overline{y} = \overline{y \cdot \overline{x}}$.

Example 9.4. If I, w, and $L_{(I,w)}$ are as in Theorem 8.2 and Definition 8.3, then $\overline{L_{(I,w)}} = L_{(\overline{I},w)}$, and applying Lemma 6.6(ii)(d) with $a = \frac{x\overline{y}}{w}$ shows that $x \cdot \overline{y} = \frac{x\overline{y}}{w}$. In particular, if $L = \mathbb{Z}\langle G\rangle$, then $\overline{L} = \mathbb{Z}\langle G\rangle$ with $^-$ having the same meaning as in Definition 6.3 for $A = \mathbb{Z}$, and with $\cdot$ being multiplication in $\mathbb{Z}\langle G\rangle$. Note that when $w \neq 1$, ideals I in $\mathbb{Z}\langle G\rangle$ do not inherit their lifted inner product from that of $\mathbb{Z}\langle G\rangle$.

Definition 9.5. A G-lattice L is **invertible** if the following three conditions all hold:

(i) $\mathrm{rank}(L) = n = \#G/2$;
(ii) L is unimodular (see Definition 2.3);
(iii) for each $m \in \mathbb{Z}_{>0}$ there exists $e_m \in L$ such that $\{\sigma e_m + mL : \sigma \in G\}$ generates the abelian group L/mL.

It is clear from the definition that invertibility is preserved under G-lattice isomorphisms. Definition 9.5 implies that L/mL is a free $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$-module of rank one for all $m > 0$. Given an ideal, it is a hard problem to decide if it is principal. But checking (iii) of Definition 9.5 is easy algorithmically; see Algorithm 10.2 below.

Lemma 9.6. *If L is a G-lattice and L is G-isomorphic to the standard G-lattice, then L is invertible.*

Proof. Parts (i) and (ii) of Definition 9.5 are easy. For (iii), observe that the group $\mathbb{Z}\langle G\rangle$ is generated by $\{\sigma 1 : \sigma \in G\}$, so the group L is generated by $\{\sigma e : \sigma \in G\}$ where e is the image of 1 under the isomorphism. Now let $e_m = e$ for all m. □

10. Determining invertibility

Fix as before a finite abelian group G of order $2n$ equipped with an element u of order 2.

Algorithm 10.2 below determines whether a G-lattice is invertible. In Proposition 10.3 we show that Algorithm 10.2 produces correct output and runs in polynomial time.

In [8] we obtain a deterministic polynomial-time algorithm on input a finite commutative ring R and a finite R-module M, decides whether there exists $y \in M$ such that $M = Ry$, and if there is, finds such a y. Applying this with $R = \mathbb{Z}\langle G\rangle/(m)$ and $M = L/mL$ gives the algorithm in the following result.

Proposition 10.1. *There is a deterministic polynomial-time algorithm that, given G, u, a G-lattice L, and $m \in \mathbb{Z}_{>0}$, decides whether there exists $e_m \in L$ such that $\{\sigma e_m + mL : \sigma \in G\}$ generates L/mL as an abelian group, and if there is, finds one.*

Algorithm 10.2. Given G, u, and a G-lattice L, the algorithm decides whether L is invertible.

(i) If $\operatorname{rank}(L) \neq n$, output "no" (and stop).
(ii) Compute the determinant of the Gram matrix for L. If it is not 1, output "no" (and stop).
(iii) Use Proposition 10.1 to determine if e_2 (in the notation of Definition 9.5(iii)) exists. If no e_2 exists, output "no" and stop. Otherwise, use Proposition 10.1 to compute $e_2 \in L$.
(iv) Compute the order q of the group $L/(\mathbb{Z}\langle G\rangle \cdot e_2)$.
(v) Use Proposition 10.1 to determine if e_q exists. If no e_q exists, output "no". Otherwise, output "yes".

Proposition 10.3. *Algorithm 10.2 is a deterministic polynomial-time algorithm that, given G, u, and a G-lattice L, decides whether L is invertible.*

Proof. If Step (ii) outputs "no" then L is not unimodular so it is not invertible. We need to check Definition 9.5(iii) for all m's in polynomial time. We show that it suffices to check two particular values of m, namely $m = 2$ and q. By Lemma 10.4, the group $L/(\mathbb{Z}\langle G\rangle \cdot e_2)$ is finite of odd order q. If no e_q exists, L is not invertible. If e_q exists, then for *all* $m \in \mathbb{Z}_{>0}$ there exists $e_m \in L$ that generates L/mL as a $\mathbb{Z}\langle G\rangle/(m)$-module, as follows. We can reduce to m being a prime power p^t, since if $\gcd(m, m') = 1$ then $L/mm'L$ is free of rank 1 over $\mathbb{Z}\langle G\rangle/(mm')$ if and only if L/mL is free of rank 1 over $\mathbb{Z}\langle G\rangle/(m)$ and $L/m'L$ is free of rank 1 over $\mathbb{Z}\langle G\rangle/(m')$. Lemma 10.4 now allows us to reduce to the case $m = p$. If p does not divide q, we can take $e_p = e_2$. If p divides q, we can take $e_p = e_q$. □

Lemma 10.4. *Suppose that L is a G-lattice, $m \in \mathbb{Z}_{>1}$, and $e \in L$. Then $\{\sigma e + mL : \sigma \in G\}$ generates L/mL as an abelian group if and only if $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is finite of order coprime to m.*

Proof. The set $\{\sigma e + mL : \sigma \in G\}$ generates L/mL as an abelian group if and only if $L = \mathbb{Z}\langle G\rangle e + mL$, and if and only if multiplication by m is surjective as a map from $L/(\mathbb{Z}\langle G\rangle \cdot e)$ to itself. Since $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is a finitely generated abelian group, this holds if and only if $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is finite of order coprime to m. □

11. Equivalent conditions for invertibility

In this section we prove Theorem 11.1, which gives equivalent conditions for invertibility.

Theorem 11.1. *If L is a G-lattice, then the following statements are equivalent:*

(a) *L is invertible;*
(b) *the map $\varphi : L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} \to \mathbb{Z}\langle G\rangle$ defined by $\varphi(x \otimes \overline{y}) = x \cdot \overline{y}$ is an isomorphism of $\mathbb{Z}\langle G\rangle$-modules, where $\cdot$ is defined in Definition 9.2;*
(c) *there is a $\mathbb{Z}\langle G\rangle$-module M such that $L \otimes_{\mathbb{Z}\langle G\rangle} M$ and $\mathbb{Z}\langle G\rangle$ are isomorphic as $\mathbb{Z}\langle G\rangle$-modules, and as a lattice L is unimodular;*
(d) *L is G-isomorphic to $L_{(I,w)}$ for some fractional $\mathbb{Z}\langle G\rangle$-ideal I and some $w \in \mathbb{Q}\langle G\rangle^*$ such that $I\overline{I} = \mathbb{Z}\langle G\rangle \cdot w$ and $\psi(w) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, with $L_{(I,w)}$ as in Definition 8.3.*

We will prove Theorem 11.1 in a series of lemmas. The equivalence of (a) and (c) says that being invertible as a G-lattice is equivalent to being both unimodular as a lattice and invertible as a $\mathbb{Z}\langle G\rangle$-module.

Definition 11.2. Suppose R is a commutative ring. An R-module is **projective** if it is a direct summand of a free R-module. An R-module M is **flat** if whenever $N_1 \hookrightarrow N_2$ is an injection of R-modules, then the induced map $M \otimes_R N_1 \to M \otimes_R N_2$ is injective.

Lemma 11.3. *Suppose that L is a $\mathbb{Z}$-free $\mathbb{Z}\langle G\rangle$-module of rank $\#G/2$, and for each $m \in \mathbb{Z}_{>0}$ there exists $e_m \in L$ such that $\{\sigma e_m + mL : \sigma \in G\}$ generates the abelian group L/mL. Then:*

(i) *there is a $\mathbb{Z}\langle G\rangle$-module M such that $L \oplus M \cong \mathbb{Z}\langle G\rangle \oplus \mathbb{Z}\langle G\rangle$, and*
(ii) *L is projective and flat as a $\mathbb{Z}\langle G\rangle$-module.*

Proof. Let $q = [L : \mathbb{Z}\langle G\rangle e_2]$. By Lemma 10.4, we have that q is finite and odd. Let $r = [L : \mathbb{Z}\langle G\rangle e_q]$. By Lemma 10.4, we have that r is finite and coprime to q. Take $a, b \in \mathbb{Z}$ such that $ar + bq = 1$. Let $N = \mathbb{Z}\langle G\rangle e_2 \oplus \mathbb{Z}\langle G\rangle e_q$ and $M = \mathbb{Z}\langle G\rangle e_2 \cap \mathbb{Z}\langle G\rangle e_q$. Since L has rank $\#G/2$ we have $N \cong \mathbb{Z}\langle G\rangle \oplus \mathbb{Z}\langle G\rangle$. Define $p : N \to L$ by $(x, y) \mapsto x + y$ and $s : L \to N$ by $x \mapsto (bqx, arx)$. Then $p \circ s$ is the identity on L. Thus, $L \oplus \ker(p) \cong N \cong \mathbb{Z}\langle G\rangle \oplus \mathbb{Z}\langle G\rangle$. Since L is a direct summand of a free module, L is projective. All projective modules are flat (by Example (1) in I.2.4 of [2]). □

Recall that the notions of fractional $\mathbb{Z}\langle G\rangle$-ideal and invertible fractional $\mathbb{Z}\langle G\rangle$-ideal were defined in Definition 8.1.

Lemma 11.4. *If I is an invertible fractional $\mathbb{Z}\langle G\rangle$-ideal, then:*

(i) *if $m \in \mathbb{Z}_{>0}$, then I/mI is isomorphic to $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$ as a $\mathbb{Z}\langle G\rangle$-module;*
(ii) *I is flat;*
(iii) *if I' is a fractional $\mathbb{Z}\langle G\rangle$-ideal, then the natural surjective map $I \otimes_{\mathbb{Z}\langle G\rangle} I' \to II'$ is an isomorphism.*

Proof. Since I is an invertible fractional $\mathbb{Z}\langle G\rangle$-ideal, there is a fractional $\mathbb{Z}\langle G\rangle$-ideal J such that $IJ = \mathbb{Z}\langle G\rangle$. Let $\mathcal{F}$ denote the partially ordered set of fractional $\mathbb{Z}\langle G\rangle$-ideals. The maps from $\mathcal{F}$ to itself defined by $f_1 : N \mapsto NI$ and $f_2 : N \mapsto NJ$ are inverse bijections that preserve inclusions. Since $f_1(\mathbb{Z}\langle G\rangle) = I$, it follows that the maximal $\mathbb{Z}\langle G\rangle$-submodules of I are exactly the $\mathfrak{m}I$ such that $\mathfrak{m}$ is a maximal ideal of $\mathbb{Z}\langle G\rangle$. By the Chinese Remainder Theorem, the map $I \to \prod_{\mathfrak{m}} I/\mathfrak{m}I$ is surjective, where the product runs over the (finitely many) maximal ideals $\mathfrak{m}$ that contain m. It follows that there exists $x \in I$ that is not contained in any $\mathfrak{m}I$. Since $\mathbb{Z}\langle G\rangle x + mI$ is a fractional ideal that is not contained in any proper submodule of I, it equals I. Thus, I/mI is isomorphic to $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$ as a $\mathbb{Z}\langle G\rangle$-module. This proves (i).

For (ii), apply (i) and Lemma 11.3(ii).

Since I is flat, the natural map

$$I \otimes_{\mathbb{Z}\langle G\rangle} I' \to I \otimes_{\mathbb{Z}\langle G\rangle} \mathbb{Q}\langle G\rangle \cong I \otimes_{\mathbb{Z}\langle G\rangle} \mathbb{Z}\langle G\rangle \otimes_{\mathbb{Z}} \mathbb{Q} \cong I \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}\langle G\rangle$$

is injective, giving (iii). □

Let $L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$. Then the inner product $\langle\ ,\ \rangle$ on L extends $\mathbb{Q}$-bilinearly to a $\mathbb{Q}$-bilinear, symmetric, positive definite inner product on $L_{\mathbb{Q}}$, and the lifted inner product $\cdot$ extends $\mathbb{Q}$-bilinearly to a $\mathbb{Q}\langle G\rangle$-bilinear map $L_{\mathbb{Q}} \times \overline{L_{\mathbb{Q}}} \to \mathbb{Q}\langle G\rangle$.

Lemma 11.5. *Suppose L is an invertible G-lattice. Then $L_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle\gamma$ for some $\gamma \in L_{\mathbb{Q}}$. For such a γ, letting $z = \gamma \cdot \overline{\gamma} \in \mathbb{Q}\langle G\rangle$ we have:*

(i) *$z \in \mathbb{Q}\langle G\rangle^*$,*
(ii) *for all $\psi \in \Psi$ we have $\psi(z) \in \mathbb{R}_{>0}$,*
(iii) *$L \cdot \overline{L} = \mathbb{Z}\langle G\rangle$,*
(iv) *if $I = \{x \in \mathbb{Q}\langle G\rangle : x\gamma \in L\}$, then $I\overline{I} = \mathbb{Z}\langle G\rangle z^{-1}$ and $L_{(I,z^{-1})} \cong L$ as G-lattices.*

Proof. By Definition 9.5(iii) and Lemma 10.4 we have that for all $m \in \mathbb{Z}_{>1}$ there exists $e_m \in L$ such that the index $i(m) = [L : \mathbb{Z}\langle G\rangle e_m]$ is finite and coprime to m. It follows that $L_{\mathbb{Q}} \cong \mathbb{Q}\langle G\rangle$ as $\mathbb{Q}\langle G\rangle$-modules. Thus, $L_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle\gamma$ for some $\gamma \in L_{\mathbb{Q}}$. Let $z = \gamma \cdot \overline{\gamma} \in \mathbb{Q}\langle G\rangle$.

For all $x, y \in \mathbb{Q}\langle G\rangle$ we have $\langle x\gamma, y\gamma\rangle = t(x\gamma \cdot \overline{y\gamma}) = t(x\overline{y}z)$. Since the inner product is symmetric, using Lemma 6.6(ii)(e) we have $\bar{z} = z$. Thus for all $\psi \in \Psi$ we have $\psi(z) = \psi(\bar{z}) = \overline{\psi(z)}$ by Lemma 7.3(i), so $\psi(z) \in \mathbb{R}$. For all $x \in \mathbb{Q}\langle G\rangle$ we have $0 \leq \langle x\gamma, x\gamma\rangle = t(x\overline{x}z) = \frac{1}{n}\sum_{\psi\in\Psi} \psi(x\overline{x}z)$ by Lemma 7.3(ii). By Lemma 7.3(vii) it follows that $\psi(z) \geq 0$ for all $\psi \in \Psi$. If $x \in \mathbb{Q}\langle G\rangle$ and $zx = 0$, then $\langle x\gamma, x\gamma\rangle = t(x\overline{x}z) = 0$, so $x = 0$. Therefore multiplication by z is an injective, and

thus surjective, map from $\mathbb{Q}\langle G\rangle$ to itself. Thus $z \in \mathbb{Q}\langle G\rangle^*$ and $\psi(z) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, by Lemma 7.3(vi). This gives (i) and (ii).

Define $L^{-1} = \{\overline{y} \in \overline{L}_{\mathbb{Q}} : L \cdot \overline{y} \subset \mathbb{Z}\langle G\rangle\}$ and let $m \in \mathbb{Z}_{>1}$. We have $L \supset \mathbb{Z}\langle G\rangle e_m \supset i(m)L$, so $e_m \in \mathbb{Q}\langle G\rangle^*\gamma$ and therefore $e_m \cdot \overline{e_m} \in \mathbb{Q}\langle G\rangle^*$. Now $i(m)(e_m \cdot \overline{e_m})^{-1}\overline{e_m} \in L^{-1}$, because for all $x \in L$ one has $i(m)x \cdot (e_m \cdot \overline{e_m})^{-1}\overline{e_m} \subset \mathbb{Z}\langle G\rangle e_m \cdot (e_m \cdot \overline{e_m})^{-1}\overline{e_m} = \mathbb{Z}\langle G\rangle$. Therefore $i(m) = e_m \cdot i(m)(e_m \cdot \overline{e_m})^{-1}\overline{e_m} \in L \cdot L^{-1} \subset \mathbb{Z}\langle G\rangle$. This is true for all $m \in \mathbb{Z}_{>1}$, so $1 \in L \cdot L^{-1}$ and $L \cdot L^{-1} = \mathbb{Z}\langle G\rangle$.

Now for $\overline{y} \in \overline{L}_{\mathbb{Q}}$ one has $\overline{y} \in \overline{L}$ if and only if $y \in L$, if and only if for all $x \in L$ one has $\langle x, y\rangle \in \mathbb{Z}$, if and only if for all $x \in L$ and $\sigma \in G$ one has $\langle x, \sigma y\rangle = \langle \sigma^{-1}x, y\rangle \in \mathbb{Z}$, if and only if for all $x \in L$ one has $x \cdot \overline{y} \in \mathbb{Z}\langle G\rangle$, if and only if $\overline{y} \in L^{-1}$. So $\overline{L} = L^{-1}$. Thus $L \cdot \overline{L} = \mathbb{Z}\langle G\rangle$, giving (iii).

If $I \subset \mathbb{Q}\langle G\rangle$ is such that $L = I\gamma$, then $I \xrightarrow{\sim} L$, $x \mapsto x\gamma$ as $\mathbb{Z}\langle G\rangle$-modules. Then $\mathbb{Z}\langle G\rangle = L \cdot \overline{L} = I\overline{I}\gamma \cdot \overline{\gamma} = I\overline{I}z$, so $I\overline{I} = \mathbb{Z}\langle G\rangle z^{-1}$. Now $\langle x\gamma, y\gamma\rangle = t(x\gamma \cdot \overline{y\gamma}) = t(x\overline{y}z) = \langle x, y\rangle_{I,z^{-1}}$ for all $x, y \in I$. Thus, $L_{(I,z^{-1})} \cong L$ as G-lattices. This gives (iv). □

We are now ready to prove Theorem 11.1.

For (a) ⇒ (d), apply Lemma 11.5 with $w = z^{-1}$.

For (d) ⇒ (b), by (d) we have $L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} = I \otimes_{\mathbb{Z}\langle G\rangle} \overline{I}$. Using Lemma 11.4(iii) we have that the composition $I \otimes \overline{I} \xrightarrow{\sim} I\overline{I} = \mathbb{Z}\langle G\rangle w \xrightarrow{\sim} \mathbb{Z}\langle G\rangle$ is an isomorphism, where the first map sends $x \otimes y$ to $x\overline{y}$ and the last map sends α to α/w. Since $x \cdot \overline{y} = x\overline{y}/w$, this gives (b).

For (b) ⇒ (c), suppose (b) holds, i.e., the map $\varphi : L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} \to \mathbb{Z}\langle G\rangle$, $x \otimes \overline{y} \mapsto x \cdot \overline{y}$ is an isomorphism of $\mathbb{Z}\langle G\rangle$-modules. Then L is unimodular, as follows. Consider the maps:

$$L \to \mathrm{Hom}_{\mathbb{Z}\langle G\rangle}(\overline{L}, \mathbb{Z}\langle G\rangle) \to \mathrm{Hom}(\overline{L}, \mathbb{Z}) \to \mathrm{Hom}(L, \mathbb{Z})$$

where the left-hand map is the $\mathbb{Z}\langle G\rangle$-module isomorphism induced by φ, defined by $x \mapsto (\bar{y} \mapsto x \cdot \overline{y})$, the middle map is $f \mapsto t \circ f$, and the right-hand map is $g \mapsto (y \mapsto g(\bar{y}))$. The latter two maps are group isomorphisms; for the middle map note that its inverse is $\hat{f} \mapsto (\overline{x} \mapsto \sum_{\sigma \in S} \hat{f}(\sigma^{-1}\overline{x})\sigma)$. The composition, which takes x to $(y \mapsto t(x \cdot \overline{y}) = \langle x, y\rangle)$, is therefore a bijection, so L is unimodular. Then (c) holds by taking $M = \overline{L}$.

For (c) ⇒ (a), by Lemma 7.3(v) we have $\mathbb{Q}\langle G\rangle \cong \prod_{j \in J} K_j$ with $\#J < \infty$ and fields K_j. Each $\mathbb{Q}\langle G\rangle$-module V is $V = \prod_{j \in J} V_j$ with each V_j a K_j-vector space. With $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$ and $W = M \otimes_{\mathbb{Z}} \mathbb{Q}$ we have

$$\prod_{j \in J}(V_j \otimes_{K_j} W_j) = V \otimes_{\mathbb{Q}\langle G\rangle} W \cong \mathbb{Q}\langle G\rangle \cong \prod_j K_j.$$

This holds if and only if for all j we have $(\dim_{K_j} V_j)(\dim_{K_j} W_j) = 1$, which holds if and only if for all j we have $\dim_{K_j} V_j = \dim_{K_j} W_j = 1$. This holds if and only if $V \cong W \cong \mathbb{Q}\langle G\rangle$ as $\mathbb{Q}\langle G\rangle$-modules. Thus, L and M may be viewed as fractional $\mathbb{Z}\langle G\rangle$-ideals in $\mathbb{Q}\langle G\rangle$, and LM is principal, so L and M are invertible fractional $\mathbb{Z}\langle G\rangle$-ideals. By Lemma 11.4(i), if I is an invertible fractional $\mathbb{Z}\langle G\rangle$-ideal, then I/mI is

cyclic as a $\mathbb{Z}\langle G\rangle$-module, for every positive integer m. Thus L/mL is cyclic as a $\mathbb{Z}\langle G\rangle$-module, so (a) holds.

This concludes the proof of Theorem 11.1.

12. Short vectors in invertible lattices

Recall that G is a group of order $2n$ equipped with an element u of order 2. The main result of this section is Theorem 12.4, which shows in particular that a G-lattice is G-isomorphic to the standard G-lattice if and only if it is invertible and has a short vector (i.e., a vector of length 1).

Definition 12.1. We will say that a vector e in an integral lattice L is **short** if $\langle e, e\rangle = 1$.

Example 12.2. The short vectors in the standard lattice of rank n are the $2n$ signed standard basis vectors $\{(0, \dots, 0, \pm 1, 0, \dots, 0)\}$. Thus, the set of short vectors in $\mathbb{Z}\langle G\rangle$ is G.

Proposition 12.3. *Suppose L is an invertible G-lattice. Then:*

(i) *if e is short, then $\{\sigma \in G : \sigma e = e\} = \{1\}$;*
(ii) *if e is short, then $\langle e, \sigma e\rangle$ is 1 if $\sigma = 1$, is -1 if $\sigma = u$, and is 0 for all other $\sigma \in G$;*
(iii) *$e \in L$ is short if and only if $e \cdot \overline{e} = 1$, with inner product $\cdot$ defined in Definition 9.2.*

Proof. Suppose $e \in L$ is short. Let $H = \{\sigma \in G : \sigma e = e\}$. For all $\sigma \in G$, by the Cauchy-Schwarz inequality we have $|\langle e, \sigma e\rangle| \le (\langle e, e\rangle\langle \sigma e, \sigma e\rangle)^{1/2} = \langle e, e\rangle = 1$, and $|\langle e, \sigma e\rangle| = 1$ if and only if e and σe lie on the same line through 0. Thus $\langle e, \sigma e\rangle \in \{1, 0, -1\}$. Then $\langle e, \sigma e\rangle = 1$ if and only if $\sigma \in H$. Also, $\langle e, \sigma e\rangle = -1$ if and only if $\sigma e = -e$ if and only if $\sigma \in Hu$. Otherwise, $\langle e, \sigma e\rangle = 0$. Thus for (i,ii), it suffices to prove $H = \{1\}$. Let $m = \#H$.

Let T be a set of coset representatives for G mod $H\langle u\rangle$ and let $S = T \cdot H$, a set of coset representatives for G mod $\langle u\rangle$. If $a = \sum_{\sigma \in S} a_\sigma \sigma \in (\mathbb{Z}/m\mathbb{Z})\langle G\rangle$ is fixed by H, then $a_{\tau\sigma} = a_\sigma$ for all $\sigma \in S$ and $\tau \in H$, so $a \in (\sum_{\tau \in H} \tau)(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$. By Definition 9.5, Theorem 11.1, and Lemma 11.4, there is a $\mathbb{Z}[H]$-module isomorphism $L/mL \cong (\mathbb{Z}/m\mathbb{Z})\langle G\rangle$. Since $e + mL$ is fixed by H, we have $e + mL \in (\sum_{\tau \in H} \tau)(L/mL)$, so $e_m \in mL + (\sum_{\tau \in H} \tau)L$. Write $e = m\varepsilon_1 + (\sum_{\tau \in H} \tau)\varepsilon_2$ with $\varepsilon_1, \varepsilon_2 \in L$. Since $\langle e, \tau\varepsilon_2\rangle = \langle \tau e, \tau\varepsilon_2\rangle = \langle e, \varepsilon_2\rangle$ for all $\tau \in H$, we have

$$1 = \langle e, e\rangle = m\langle e, \varepsilon_1\rangle + \sum_{\tau \in H} \langle e, \tau\varepsilon_2\rangle = m\langle e, \varepsilon_1 + \varepsilon_2\rangle \equiv 0 \mod m.$$

Thus, $m = 1$ as desired. Part (iii) follows directly from (ii) and Definition 9.2. □

This enables us to prove the following result.

Theorem 12.4. *Suppose L is a G-lattice. Then:*

(i) *if L is invertible, then the map*

$$\{G\text{-isomorphisms } \mathbb{Z}\langle G\rangle \to L\} \to \{\text{short vectors of } L\}$$

that sends f to $f(1)$ is bijective;

(ii) *if $e \in L$ is short and L is invertible, then $\{\sigma e : \sigma \in G\}$ generates the abelian group L;*

(iii) *L is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if L is invertible and has a short vector;*

(iv) *if $e \in L$ is short and L is invertible, then the map $G \to \{\text{short vectors of } L\}$ defined by $\sigma \mapsto \sigma e$ is bijective.*

Proof. For (i), that $f(1)$ is short is clear. Injectivity of the map $f \mapsto f(1)$ follows from $\mathbb{Z}\langle G\rangle$-linearity of G-isomorphisms. For surjectivity, suppose $e \in L$ is short. Proposition 12.3(ii) says that $\{\sigma e\}_{\sigma\in S}$ is an orthonormal basis for L. Parts (ii) and (i) now follow, where the G-isomorphism f is defined by $x \mapsto xe$ for all $x \in \mathbb{Z}\langle G\rangle$. Part (iii) follows from (i) and Lemma 9.6. Part (iv) is trivial for $\mathbb{Z}\langle G\rangle$, and L is G-isomorphic to $\mathbb{Z}\langle G\rangle$, so we have (iv). □

13. Tensor products of G-lattices

Recall that G is a finite abelian group with an element u of order 2. We will define the tensor product of invertible G-lattices, and derive some properties.

Definition 13.1. Suppose that L and M are invertible G-lattices. Define the $\mathbb{Z}\langle G\rangle$-bilinear map

$$\cdot : (L \otimes_{\mathbb{Z}\langle G\rangle} M) \times (\overline{L} \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}) \to \mathbb{Z}\langle G\rangle, \quad (a, \overline{b}) \mapsto a \cdot \overline{b}$$

by letting $(x \otimes v) \cdot (\overline{y} \otimes \overline{w}) = (x \cdot \overline{y})(v \cdot \overline{w})$ for all $x, y \in L$ and $v, w \in M$ and extending $\mathbb{Z}\langle G\rangle$-bilinearly. Take $\overline{L \otimes_{\mathbb{Z}\langle G\rangle} M}$ to be $\overline{L} \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}$, with $\overline{x \otimes v} = \overline{x} \otimes \overline{v}$.

Example 13.2. Let $L = L_{(I_1,w_1)}$ and $M = L_{(I_2,w_2)}$ where I_1, I_2 are fractional $\mathbb{Z}\langle G\rangle$-ideals, $w_1, w_2 \in \mathbb{Q}\langle G\rangle^*$ are such that $\psi(w_i) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, and $I_i\overline{I_i} = \mathbb{Z}\langle G\rangle w_i$ for $i = 1, 2$. Then $L \otimes_{\mathbb{Z}\langle G\rangle} M$ may be identified with I_1I_2 via Lemma 11.4, and $\overline{L \otimes_{\mathbb{Z}\langle G\rangle} M}$ with $\overline{I_1I_2}$, and the dot product $I_1I_2 \times \overline{I_1I_2} \to \mathbb{Z}\langle G\rangle$ from Definition 13.1 becomes $a \cdot \overline{b} = a\overline{b}/(w_1w_2)$ as in Example 9.4. This is precisely the lifted inner product of the G-lattice $L_{(I_1I_2,w_1w_2)}$ (which is invertible by Theorem 11.1). We thus have

$$L_{(I_1,w_1)} \otimes_{\mathbb{Z}\langle G\rangle} L_{(I_2,w_2)} = L_{(I_1I_2,w_1w_2)}. \tag{13.3}$$

Theorem 13.4. *Let L and M be invertible G-lattices. Then $L \otimes_{\mathbb{Z}\langle G\rangle} M$ is an invertible G-lattice with inner product $\langle a, b\rangle = t(a \cdot \overline{b})$, where the dot product is defined in Definition 13.1 and equals the lifted inner product for this G-lattice.*

Proof. By Theorem 11.1 we may assume that $L = L_{(I_1,w_1)}$ and $M = L_{(I_2,w_2)}$ where I_1, I_2 are fractional $\mathbb{Z}\langle G\rangle$-ideals, $w_1, w_2 \in \mathbb{Q}\langle G\rangle^*$ are such that $\psi(w_i) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, and $I_i\overline{I_i} = \mathbb{Z}\langle G\rangle w_i$ for $i = 1, 2$. In this case, we already checked the theorem in Example 13.2. □

Proposition 13.5. *Suppose that L, M, and N are invertible G-lattices. Then we have the following G-isomorphisms:*

(i) $L \otimes_{\mathbb{Z}\langle G\rangle} M \cong M \otimes_{\mathbb{Z}\langle G\rangle} L$,
(ii) $(L \otimes_{\mathbb{Z}\langle G\rangle} M) \otimes_{\mathbb{Z}\langle G\rangle} N \cong L \otimes_{\mathbb{Z}\langle G\rangle} (M \otimes_{\mathbb{Z}\langle G\rangle} N)$,
(iii) $L \otimes_{\mathbb{Z}\langle G\rangle} \mathbb{Z}\langle G\rangle \cong L$,
(iv) $L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} \cong \mathbb{Z}\langle G\rangle$.

Proof. By Theorem 11.1 we may reduce to the case where the invertible G-lattices are of the form $L_{(I,w)}$. Then (13.3) immediately gives (i) and (ii). For (iii) and (iv), note that $\mathbb{Z}\langle G\rangle = L_{(\mathbb{Z}\langle G\rangle,1)}$, and if $L = L_{(I,w)}$ then $\overline{L} \cong L_{(\bar{I},w)} \cong L_{(\bar{I}w^{-1},w^{-1})} = L_{(I^{-1},w^{-1})}$. □

Remark 13.6. One can extend parts (i), (ii), and (iii) of Proposition 13.5 to general G-lattices, by replacing $L \otimes_{\mathbb{Z}\langle G\rangle} M$ by its image in $L_{\mathbb{Q}} \otimes_{\mathbb{Q}\langle G\rangle} M_{\mathbb{Q}}$. That image is a G-lattice with lifted inner product given by the same formula.

14. The Witt-Picard group

As before, G is a finite abelian group of order $2n$ equipped with an element u of order 2.

Definition 14.1. We define

$$\mathrm{WPic}_{\mathbb{Z}\langle G\rangle} = \{[L] : L \text{ is an invertible } G\text{-lattice}\},$$

where the symbols $[L]$ are chosen so that $[L] = [M]$ if and only if L and M are G-isomorphic.

Theorem 14.2. *The set* $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ *is an abelian group, with group operation defined by* $[L] \cdot [M] = [L \otimes_{\mathbb{Z}\langle G\rangle} M]$*, with identity element* $[\mathbb{Z}\langle G\rangle]$*, and with* $[L]^{-1} = [\overline{L}]$.

Proof. This follows immediately from Theorem 13.4 and Proposition 13.5. □

Corollary 14.3. *Suppose that L and M are invertible G-lattices. Then L and M are G-isomorphic if and only if $L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}$ and $\mathbb{Z}\langle G\rangle$ are G-isomorphic.*

Proof. This follows immediately from Theorem 14.2. □

The following description of $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ is reminiscent of the definition of class groups in algebraic number theory.

Proposition 14.4. *Let $\mathcal{I}_{\mathbb{Z}\langle G\rangle}$ denote the group of invertible fractional $\mathbb{Z}\langle G\rangle$-ideals. Then the group* $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ *is isomorphic to the quotient of the group*

$$\{(I, w) \in \mathcal{I}_{\mathbb{Z}\langle G\rangle} \times \mathbb{Q}\langle G\rangle^* : I\overline{I} = \mathbb{Z}\langle G\rangle w \text{ and } \psi(w) \in \mathbb{R}_{>0} \text{ for all } \psi \in \Psi\}$$

by its subgroup $\{(\mathbb{Z}\langle G\rangle v, v\overline{v}) : v \in \mathbb{Q}\langle G\rangle^*\}$.

Proof. Define the map by $(I, w) \mapsto [L_{(I,w)}]$. Surjectivity follows from Theorem 11.1, and the kernel is the desired subgroup by Theorem 8.5. □

Just as for the class group, we have:

Theorem 14.5. *The group* $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ *is finite.*

Proof. If L is an invertible G-lattice and $\{b_1, \ldots, b_n\}$ is an LLL-reduced basis, and for $\sigma \in G$ we have $\sigma(b_i) = \sum_{j=1}^{n} a_{ij}^{(\sigma)} b_j$ with $a_{ij}^{(\sigma)} \in \mathbb{Z}$, then $|\langle b_i, b_j\rangle| \leq 2^{n-1}$ and $|a_{ij}^{(\sigma)}| \leq 3^{n-1}$ for all i, j, and σ, by Proposition 3.4(iii) and (iv). Thus there are only finitely many possibilities for $((\langle b_i, b_j\rangle)_{i,j=1}^{n}, (a_{ij}^{(\sigma)})_{i,j=1,\ldots,n;\sigma\in G})$. If L' is also an invertible G-lattice with LLL-reduced basis $\{b'_1, \ldots, b'_n\}$, and if we have $\langle b_i, b_j\rangle = \langle b'_i, b'_j\rangle$ and $a_{ij}^{(\sigma)} = a_{ij}^{\prime(\sigma)}$ for all i, j, and σ, then the group isomorphism $L \to L'$, $b_i \mapsto b'_i$ is an isomorphism of G-lattices. The finiteness of $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ now follows. □

We call $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ the **Witt-Picard group** of $\mathbb{Z}\langle G\rangle$. The reason for the nomenclature lies in Theorem 11.1. If R is a commutative ring, an invertible R-module is an R-module L for which there exists an R-module M with $L \otimes_R M \cong R$. The Picard group Pic_R is the set of invertible R-modules up to isomorphism, where the group operation is tensoring over R. This addresses the module structure, while Witt rings reflect the structure as a unimodular lattice.

Algorithm 14.6. Given invertible G-lattices L and M equipped with LLL-reduced bases, the algorithm outputs $L \otimes_{\mathbb{Z}\langle G\rangle} M$ with an LLL-reduced basis and an $n \times n \times n$ array of integers to describe the multiplication map $L \times M \to L \otimes_{\mathbb{Z}\langle G\rangle} M$.

(i) Compute the tensor product $L \otimes_{\mathbb{Z}\langle G\rangle} M$ and its lattice structure and multiplication map $L \times M \to L \otimes_{\mathbb{Z}\langle G\rangle} M$.
(ii) Compute an LLL-reduced basis for $L \otimes_{\mathbb{Z}\langle G\rangle} M$.

One way to perform step (i) in Algorithm 14.6 is to use Proposition 10.1 (with $m = 2$) in order to realize L and M as $L_{I,w}$ and $L_{I',w'}$, and take the products II' and ww'. Another (probably less efficient) option is to directly use the definition of tensor product, i.e., compute $L \otimes_{\mathbb{Z}\langle G\rangle} M$ as

$$(L \otimes_{\mathbb{Z}} M)/(\sum_{i,j,\sigma} \mathbb{Z}(\sigma b_i \otimes b'_j - b_i \otimes \sigma b'_j))$$

where $L \otimes_{\mathbb{Z}} M = \bigoplus_{i,j} \mathbb{Z}(b_i \otimes b'_j)$. With either choice, Algorithm 14.6 runs in polynomial time.

Applying Algorithm 14.6 gives the following polynomial-time algorithm.

Algorithm 14.7. Given G and u as usual, G-lattices L and L' equipped with LLL-reduced bases, a positive integer m, and elements $d \in L/mL$ and $d' \in L'/mL'$, the algorithm computes $L \otimes_{\mathbb{Z}\langle G\rangle} L'$ and the element $d \otimes d' \in (L \otimes L')/m(L \otimes L')$.

(i) Apply Algorithm 14.6 to compute $L \otimes_{\mathbb{Z}\langle G\rangle} L'$.
(ii) Lift d to L and d' to L', and then apply the map

$$L \times L' \to L \otimes_{\mathbb{Z}\langle G\rangle} L' \to (L \otimes L')/m(L \otimes L').$$

For all G, u, and $m \in \mathbb{Z}_{>0}$, there is a bound on the runtime of the previous algorithm that holds uniformly for all L, L', d, and d', and this bound is polynomial in the length of the data specifying G, u, and m.

Applying basis reduction, and iterating Algorithm 14.7 using an addition chain for r, gives the following polynomial-time algorithm. It replaces the polynomial chains in §7.4 of the Gentry-Szydlo paper [3].

Algorithm 14.8. Given G, u, a G-lattice L, positive integers m and r, and $d \in L/mL$, the algorithm computes $L^{\otimes r}$ and $d^{\otimes r} \in L^{\otimes r}/mL^{\otimes r}$.

Note that it is $\log(r)$ and not r that enters in the runtime. This means that very high powers of lattices can be computed without coefficient blow-up, thanks to the basis reduction that takes place in Algorithm 14.6(ii). The fact that this is possible was one of the crucial ideas of Gentry and Szydlo.

15. The extended tensor algebra Λ

The extended tensor algebra Λ is a single algebraic structure that comprises all rings and lattices that our main algorithm needs, including their inner products.

Suppose L is an invertible G-lattice. Letting $L^{\otimes 0} = \mathbb{Z}\langle G\rangle$ and letting $L^{\otimes m} = L \otimes_{\mathbb{Z}\langle G\rangle} \cdots \otimes_{\mathbb{Z}\langle G\rangle} L$ (with m L's) and $L^{\otimes(-m)} = \overline{L}^{\otimes m} = \overline{L} \otimes_{\mathbb{Z}\langle G\rangle} \cdots \otimes_{\mathbb{Z}\langle G\rangle} \overline{L}$ for all $m \in \mathbb{Z}_{>0}$, define the extended tensor algebra

$$\Lambda \;=\; \bigoplus_{i\in\mathbb{Z}} L^{\otimes i} \;=\; \ldots \oplus \overline{L}^{\otimes 3} \oplus \overline{L}^{\otimes 2} \oplus \overline{L} \oplus \mathbb{Z}\langle G\rangle \oplus L \oplus L^{\otimes 2} \oplus L^{\otimes 3} \oplus \ldots$$

("extended" because we extend the usual notion to include negative exponents $L^{\otimes(-m)}$). Each $L^{\otimes i}$ is an invertible G-lattice, and represents $[L]^i$. For simplicity, we denote $L^{\otimes i}$ by L^i. For all $j \in \mathbb{Z}$ we have $\overline{L^j} = \overline{L}^j = L^{-j}$. Note that computing the G-lattice $L^{-1} = \overline{L}$ is trivial; just compose the G-action map $G \to \mathrm{GL}(n,\mathbb{Z})$ with the map $G \to G$, $\sigma \mapsto \overline{\sigma}$. The ring structure on Λ is defined as the ring structure on the tensor algebra, supplemented with the lifted inner product $\cdot$ of Definition 9.2. Let $\Lambda_{\mathbb{Q}} = \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 15.1. (i) *The extended tensor algebra Λ is a commutative ring containing $\mathbb{Z}\langle G\rangle$ as a subring;*

(ii) *for all $j \in \mathbb{Z}$, the action of G on L^j becomes multiplication in Λ;*

(iii) *Λ has an involution $x \mapsto \overline{x}$ extending both the involution of $\mathbb{Z}\langle G\rangle$ and the map $L \xrightarrow{\sim} \overline{L}$;*

(iv) *if $j \in \mathbb{Z}$, then the lifted inner product $\cdot : L^j \times \overline{L^j} \to \mathbb{Z}\langle G\rangle$ becomes multiplication in Λ, with $\overline{L^j} = \overline{L}^j$;*

(v) *if $j \in \mathbb{Z}$, then for all $x, y \in L^j$ we have $\langle x, y\rangle = t(x\overline{y})$;*

(vi) *if $j \in \mathbb{Z}$ and $e \in L^j$ is short, then $\overline{e} = e^{-1}$ in L^{-j};*

(vii) *if γ is as in Lemma 11.5, then $\gamma \in \Lambda_{\mathbb{Q}}^*$, one has $L^i_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle\gamma^i$ for all $i \in \mathbb{Z}$, and $\Lambda_{\mathbb{Q}}$ may be identified with the Laurent polynomial ring $\mathbb{Q}\langle G\rangle[\gamma, \gamma^{-1}]$.*

(viii) *if $e \in L$ is short, then $\Lambda = \mathbb{Z}\langle G\rangle[e, e^{-1}]$.*

Proof. The proof is straightforward. It is best to begin with (vii). □

All computations in Λ and in $\Lambda/m\Lambda = \bigoplus_{i\in\mathbb{Z}} L^i/mL^i$ with $m \in \mathbb{Z}_{>0}$ that occur in our algorithms are done with homogeneous elements only, where the set of homogeneous elements of Λ is $\bigcup_{i\in\mathbb{Z}} L^i$.

If A is a commutative ring, let $\mu(A)$ denote the subgroup of A^* consisting of the roots of unity, i.e., the elements of finite order. The following result will allow us to construct a polynomial-time algorithm to find k-th roots of short vectors, when they exist.

Proposition 15.2. *Suppose L is an invertible G-lattice, $r \in \mathbb{Z}_{>0}$, and ν is a short vector in the G-lattice L^r. Let $A = \Lambda/(\nu - 1)$. Identifying $\bigoplus_{i=0}^{r-1} L^i \subset \Lambda$ with its image in A, we can view $A = \bigoplus_{i=0}^{r-1} L^i$ as a $\mathbb{Z}/r\mathbb{Z}$-graded ring. Then:*

(i) $G \subseteq \mu(A) \subseteq \bigcup_{i=0}^{r-1} L^i$,
(ii) $\{e \in L : e \cdot \bar{e} = 1\} = \mu(A) \cap L$,
(iii) *$|\mu(A)|$ is divisible by $2n$ and divides $2nr$,*
(iv) *the degree map $\mu(A) \to \mathbb{Z}/r\mathbb{Z}$ that takes $e \in \mu(A)$ to j such that $e \in L^j$ is surjective if and only if $\mu(A) \cap L \neq \emptyset$, and*
(v) *there exists $e \in L$ for which $e \cdot \bar{e} = 1$ if and only if $\#\mu(A) = 2nr$.*

Proof. Since the ideal $(\overline{\nu} - 1) = (\nu^{-1} - 1) = (1 - \nu) = (\nu - 1)$, the map $a \mapsto \overline{a}$ induces an involution on A.

Next we show that the natural map $\bigoplus_{i=0}^{r-1} L^i \to \Lambda/(\nu - 1) = A$ is bijective. For surjectivity, by Proposition 15.1(vi) we have $\nu L^j = L^{j+r}$ for all $j \in \mathbb{Z}$, and thus L^{j+r} and L^j have the same image under the natural map $\Lambda \to \Lambda/(\nu - 1) = A$. For injectivity, suppose $0 \neq a = \sum_{i=h}^{j} a_i \in \Lambda$ with $h \leq j$, with all $a_i \in L^i$, and with $a_h \neq 0$ and $a_j \neq 0$. Then $(\nu - 1)a = \sum_{i=h}^{j+r} b_i$ with $b_i \in L^i$ where $b_h = -a_h \neq 0$ and $b_{j+r} = \nu a_j \neq 0$, and therefore $(\nu - 1)a \notin \bigoplus_{i=0}^{r-1} L^i$. Hence we have $(\nu - 1)\Lambda \cap \bigoplus_{i=0}^{r-1} L^i = \{0\}$.

Recall that Ψ is the set of $\mathbb{C}$-algebra homomorphisms from $\mathbb{C}\langle G\rangle$ to $\mathbb{C}$. Letting $A_{\mathbb{Q}} = A \otimes_{\mathbb{Z}} \mathbb{Q}$, we have $A_{\mathbb{Q}} = \Lambda_{\mathbb{Q}}/(\nu - 1)\Lambda_{\mathbb{Q}}$ and $\Lambda_{\mathbb{Q}} = \bigoplus_{i\in\mathbb{Z}} L^i_{\mathbb{Q}}$. Since L is invertible, by Lemma 11.5 there exists $\gamma \in L_{\mathbb{Q}}$ such that $L_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle \cdot \gamma$ with $z = \gamma\overline{\gamma} \in \mathbb{Q}\langle G\rangle^*$ and $\psi(z) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$. By Proposition 15.1(vii) we have $\gamma \in L^*_{\mathbb{Q}}$, and $L^j_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle \cdot \gamma^j$ for all $j \in \mathbb{Z}$, and $\Lambda_{\mathbb{Q}} = \bigoplus_{i\in\mathbb{Z}} L^i_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle[\gamma, \gamma^{-1}]$. Thus, there exists $\delta \in \mathbb{Q}\langle G\rangle^*$ such that $\nu = \delta\gamma^r$. The set of ring homomorphisms from A to $\mathbb{C}$ can be identified with the set of ring homomorphisms from $A_{\mathbb{Q}}$ to $\mathbb{C}$, which is $\{\text{ring homomorphisms } \varphi : \Lambda_{\mathbb{Q}} \to \mathbb{C} : \varphi(\nu) = 1\}$. The latter set can be identified with $\{(\psi, \zeta) : \psi \in \Psi, \zeta \in \mathbb{C}^*, \psi(\delta)\zeta^r = 1\}$ via the map $\varphi \mapsto (\varphi|_{\mathbb{Q}\langle G\rangle}, \varphi(\gamma))$ and its inverse $(\psi, \zeta) \mapsto (\sum_i a_i\gamma^i \mapsto \sum_i \psi(a_i)\zeta^i)$, and has size $nr = \dim_{\mathbb{Q}}(A_{\mathbb{Q}})$. Since $1 = \nu\overline{\nu} = (\delta\gamma^r)\overline{(\delta\gamma^r)} = \delta\overline{\delta}z^r$, we have $\psi(\delta)\overline{\psi(\delta)}\psi(z)^r = 1 = \psi(\delta)\overline{\psi(\delta)}(\zeta\overline{\zeta})^r$, so $\psi(z)^r = (\zeta\overline{\zeta})^r$. Since $\psi(z) \in \mathbb{R}_{>0}$, we have $\psi(z) = \zeta\overline{\zeta}$. Since $\overline{\gamma} = z\gamma^{-1}$, we now have $\varphi(\overline{\gamma}) = \varphi(z)\zeta^{-1} = \overline{\zeta} = \overline{\varphi(\gamma)}$. By Lemma 7.3(i) we have $\psi(\bar{\alpha}) = \overline{\psi(\alpha)}$ for all $\alpha \in \mathbb{Q}\langle G\rangle$.

Since $A_{\mathbb{Q}}$ is generated as a ring by $\mathbb{Q}\langle G\rangle$ and γ, it follows that $\varphi(\bar{\alpha}) = \overline{\varphi(\alpha)}$ for all $\alpha \in A_{\mathbb{Q}}$ and all ring homomorphisms $\varphi : A_{\mathbb{Q}} \to \mathbb{C}$.

Applying 7.1 with to the commutative $\mathbb{Q}$-algebra $A_{\mathbb{Q}}$ shows that $\bigcap_\varphi \ker \varphi = 0$.

Let $E = \{e \in A : e\overline{e} = 1\}$, a subgroup of A^*.

If $e \in \mu(A)$, then $\varphi(e)$ is a root of unity in $\mathbb{C}$ for all ring homomorphisms $\varphi : A \to \mathbb{C}$, so $1 = \varphi(e)\overline{\varphi(e)} = \varphi(e)\varphi(\overline{e}) = \varphi(e\overline{e})$. Since $\bigcap_\varphi \ker \varphi = 0$, we have $e\overline{e} = 1$. Thus, $\mu(A) \subseteq E$.

Conversely, suppose $e \in E$. Write $e = \sum_{i=0}^{r-1} \varepsilon_i$ with $\varepsilon_i \in L^i$, so $\overline{e} = \sum_{i=0}^{r-1} \overline{\varepsilon}_i$ with $\overline{\varepsilon}_i \in L^{-i} = L^{r-i}$ in A. We have $1 = e\overline{e} = \sum_{i=0}^{r-1} \varepsilon_i\overline{\varepsilon}_i$, the degree 0 piece of $e\overline{e}$. Applying the map t of Definition 6.2 and using (9.3) we have $1 = \sum_{i=0}^{r-1} \langle \varepsilon_i, \varepsilon_i\rangle$. It follows that there exists j such that $\langle \varepsilon_j, \varepsilon_j\rangle = 1$, and $\varepsilon_i = 0$ if $i \neq j$. Thus, $E \subseteq \bigcup_{i=0}^{r-1} \{e \in L^i : \langle e, e\rangle = 1\}$, giving (i). By Proposition 12.3(iii) and Example 12.2 we have $E \cap \mathbb{Z}\langle G\rangle = G$, so $\mu(\mathbb{Z}\langle G\rangle) = G$.

The degree map from E to $\mathbb{Z}/r\mathbb{Z}$ that takes $e \in E$ to j such that $e \in L^j$ is a group homomorphism with kernel $E \cap \mathbb{Z}\langle G\rangle = G$. Therefore, $\#E$ divides $\#G\#(\mathbb{Z}/r\mathbb{Z}) = 2nr$. Thus, $E \subseteq \mu(A) \subseteq E$, so $E = \mu(A)$ and we have (ii) and (iii). The degree map is surjective if and only if $\#\mu(A) = 2nr$, and if and only if 1 is in the image, i.e., if and only if $\mu(A) \cap L \neq \emptyset$. This gives (iv). Part (v) now follows from (ii). □

Remark 15.3. In the proof of Proposition 15.2 we showed that $\mu(\mathbb{Z}\langle G\rangle) = G$.

16. Short vectors

Recall that G is a finite abelian group of order $2n$ equipped with an element u of order 2. The main result of this section is Algorithm 16.4.

Definition 16.1. The exponent of a finite group H is the least positive integer k such that $\sigma^k = 1$ for all $\sigma \in H$.

The exponent of a finite group H divides $\#H$ and has the same prime factors as $\#H$.

Definition 16.2. Let k denote the exponent of G.

By Theorem 12.4, the G-isomorphisms $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ for a G-lattice L are in one-to-one correspondence with the short vectors of L, and if a short $e \in L$ exists, then the short vectors of L are exactly the $2n$ vectors $\{\sigma e : \sigma \in G\}$. With k the exponent of G, we have $(\sigma e)^k = \sigma^k e^k = e^k$ in Λ. Hence for invertible L, all short vectors in L have the same k-th power $e^k \in \Lambda$. At least philosophically, it is easier to find things that are uniquely determined. We look for e^k first, and then recover e from it.

The n of [3] is an odd prime, so the group exponent $k = 2n$, and $\mathbb{Z}\langle G\rangle$ embeds in $\mathbb{Q}(\zeta_n) \times \mathbb{Q}$, where $\zeta_n \in \mathbb{C}^*$ is a primitive n-th root of unity. Since the latter is a product of only two number fields, the number of zeros of $X^{2n} - v^{2n}$ is at most $(2n)^2$, and the Gentry-Szydlo method for finding v from v^{2n} is sufficiently efficient. If one wants to generalize [3] to the case where n is not prime, then the smallest t such that

$\mathbb{Z}\langle G\rangle$ embeds in $F_1 \times \ldots \times F_t$ with number fields F_i can be as large as n. Given ν, the number of zeros of $X^k - \nu$ could be as large as k^t. Finding e such that $\nu = e^k$ then requires a more efficient algorithm, which we attain with Algorithm 16.4 below.

An **order** is a commutative ring A whose additive group is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$. We specify an order by saying how to multiply any two vectors in a given basis. In [9] we prove the following result, and give the associated algorithm.

Proposition 16.3. *There is a deterministic polynomial-time algorithm that, given an order A, determines a set of generators for the group $\mu(A)$ of roots of unity in A^*.*

Algorithm 16.4. Given G, u, an invertible G-lattice L, and $\nu \in L^k$ given as a sum of products of k factors from L, with k the exponent of G, the algorithm determines whether there exists $e \in L$ such that $\nu = e^k$ and $e \cdot \bar{e} = 1$, and if so, finds one.

(i) Compute the order $A = \Lambda/(\nu - 1)$.
(ii) Check whether $\nu\overline{\nu} = 1$. If $\nu\overline{\nu} \neq 1$, output "no e exists". If $\nu\overline{\nu} = 1$, apply Proposition 16.3 to compute generators for $\mu(A)$ with $A = \Lambda/(\nu - 1)$.
(iii) Apply the degree map $\mu(A) \to \mathbb{Z}/k\mathbb{Z}$ from Proposition 15.2(iv) to the generators, and check whether the images generate $\mathbb{Z}/k\mathbb{Z}$. If they do not, output "no e exists"; if they do, compute an element $e \in \mu(A)$ whose image under the degree map is 1.
(iv) Check whether $\nu = e^k$. If not, output "no e exists". If so, output e.

In step (ii), one could equivalently check whether $\langle \nu, \nu \rangle = 1$.

Proposition 16.5. *Algorithm 16.4 is a deterministic polynomial-time algorithm that, given G, u, an invertible G-lattice L, and $\nu \in L^k$, with k the exponent of G, determines whether there exists $e \in L$ such that $\nu = e^k$ and $e \cdot \bar{e} = 1$, and if so, finds one.*

Proof. We apply Proposition 15.2 with $r = k$. Suppose Step (iii) produces $e \in \mu(A)$ of degree 1. Then $e \in \mu(A) \cap L = \{\varepsilon \in L : \varepsilon \cdot \bar{\varepsilon} = 1\}$ by Proposition 15.2(ii). By Proposition 12.3(iii), this set is the set of short vectors in L. By Theorem 12.4(iv), if a short $\varepsilon \in L$ exists, then the short vectors in L are exactly the $2n$ vectors $\{\sigma\varepsilon : \sigma \in G\}$, which all have the same k-th power since k is the exponent of G. By this and Proposition 15.2(iv), if any step fails then the desired e does not exist. The algorithm runs in polynomial time since $\#\mu(A) = 2nk \leq (2n)^2$ by Proposition 15.2(v). □

17. Finding auxiliary prime powers

In this section we present an algorithm to find auxiliary prime powers ℓ and m. To bound the runtime, we use Heath-Brown's version of Linnik's theorem in analytic number theory.

Recall that G is a finite abelian group equipped with an element u of order 2, and k is the exponent of G.

Definition 17.1. For $m \in \mathbb{Z}_{>0}$ let $k(m)$ denote the exponent of the unit group $(\mathbb{Z}\langle G\rangle/(m))^*$.

Lemma 17.2. *Suppose p is a prime number and $j \in \mathbb{Z}_{>0}$. Then:*

(i) $(\mathbb{Z}/p^j\mathbb{Z})^* \subset (\mathbb{Z}\langle G\rangle/(p^j))^*$;
(ii) *if p is odd, then the exponent of $(\mathbb{Z}/p^j\mathbb{Z})^*$ is $(p-1)p^{j-1}$;*
(iii) *if $p \equiv 1 \bmod k$, then $k(p^j) = (p-1)p^{j-1}$.*

Proof. Parts (i) and (ii) are easy. For (iii), we proceed by induction on j. If $p \equiv 1 \bmod k$, then p is odd. We first take $j = 1$. The map $x \mapsto x^p$ is a ring endomorphism of $\mathbb{Z}\langle G\rangle/(p)$ and is the identity on G, since the exponent k divides $p-1$. Since G generates the ring, the map is the identity and therefore $x^p = x$ for all $x \in \mathbb{Z}\langle G\rangle/(p)$ and $x^{p-1} = 1$ for all $x \in (\mathbb{Z}\langle G\rangle/(p))^*$.

Now suppose $j > 1$. Suppose $x \in \mathbb{Z}\langle G\rangle$ maps to a unit in $\mathbb{Z}\langle G\rangle/(p^j)$. By the induction hypothesis, $x^{(p-1)p^{j-2}} \equiv 1 \bmod p^{j-1}$. Thus, $x^{(p-1)p^{j-2}} = 1 + p^{j-1}v$ for some $v \in \mathbb{Z}\langle G\rangle$. Since $(j-1)p \geq j$ we have

$$x^{(p-1)p^{j-1}} = (1 + p^{j-1}v)^p = 1 + \binom{p}{1}p^{j-1}v + \cdots + p^{(j-1)p}v^p \equiv 1 \mod p^j.$$

Thus, $k(p^j)$ divides $(p-1)p^{j-1}$ for all $j \in \mathbb{Z}_{>0}$. Part (iii) now follows from (i) and (ii). □

Theorem 17.3 (Heath-Brown, Theorem 6 of [4])**.** *There is an effective constant $c > 0$ such that if $a, t \in \mathbb{Z}_{>0}$ and $\gcd(a,t) = 1$, then the smallest prime p such that $p \equiv a \bmod t$ is at most $ct^{5.5}$.*

Algorithm 17.4. Given positive integers n and k with k even, the algorithm produces prime powers $\ell = p^r$ and $m = q^s$ with $\ell, m \geq 2^{n/2} + 1$ such that $p \equiv q \equiv 1 \bmod k$ and and $\gcd(\varphi(\ell), \varphi(m)) = k$, where φ is Euler's phi function.

(i) Try $p = k+1, 2k+1, 3k+1, \ldots$ until the least prime $p \equiv 1 \bmod k$ is found.
(ii) Find the smallest $r \in \mathbb{Z}_{>0}$ such that $p^r \geq 2^{n/2} + 1$.
(iii) Try $q = p+k, p+2k, \ldots$ until the least prime $q \equiv 1 \bmod k$ such that $\gcd((p-1)p, q-1) = k$ is found.
(iv) Find the smallest $s \in \mathbb{Z}_{>0}$ such that $q^s \geq 2^{n/2} + 1$.
(v) Let $\ell = p^r$ and $m = q^s$.

Proposition 17.5. *Algorithm 17.4 runs in time $(n+k)^{O(1)}$.*

Proof. Algorithm 17.4 takes as input $n, k \in \mathbb{Z}_{>0}$ with k even, and computes positive integers r and s and primes p and q such that:

- $p \equiv q \equiv 1 \bmod k$,
- $\gcd((p-1)p^{r-1}, (q-1)q^{s-1}) = k$,
- $p^r \geq 2^{n/2} + 1$, and
- $q^s \geq 2^{n/2} + 1$.

We next show that Algorithm 17.4 terminates, with correct output, in the claimed time. By Theorem 17.3 above, the prime p found by Algorithm 17.4 satisfies $p \leq ck^{5.5}$ with an effective constant $c > 0$. Primality testing can be done by trial division. If

$p-1 = k_1k_2$ with every prime divisor of k_1 also dividing k and with $\gcd(k_2, k) = 1$, then to have $\gcd((p-1)p, q-1) = k$ it suffices to have $q \equiv 2 \bmod p$ and $q \equiv 1+k \bmod k_1$ and $q \equiv 2 \bmod k_2$. This gives a congruence $q \equiv a \bmod p(p-1)$ for some a with $\gcd(a, p(p-1)) = 1$. Theorem 17.3 implies that Algorithm 17.4 produces a prime q with the desired properties and satisfying $q \leq c(p^2)^{5.5} \leq c(ck^{5.5})^{11} = c^{12}k^{60.5}$. The upper bounds on p and q imply that Algorithm 17.4 runs in time $(n+k)^{O(1)}$. $\square$

Remark 17.6. In practice, Algorithm 17.4 is *much* faster than implied by the proof of Proposition 17.5; Theorem 17.3 is unnecessarily pessimistic, and in practice one does not need to find a prime q that is congruent to 2 mod pk_2 and to $1+k$ mod k_1. In work in progress, we get better bounds for the runtime of our main algorithm, and avoid using the theorem of Heath-Brown or Algorithm 17.4, by generalizing our theory to the setting of "CM orders".

Algorithm 17.4 immediately yields the following algorithm.

Algorithm 17.7. Given G and u, the algorithm produces prime powers ℓ and m such that $\ell, m \geq 2^{n/2}+1$ and $\gcd(k(\ell), k(m)) = k$, where k is the exponent of G, and produces the values of $k(\ell)$ and $k(m)$.

(i) Compute n and k.
(ii) Run Algorithm 17.4 to compute prime powers $\ell = p^r$ and $m = q^s$ with $\ell, m \geq 2^{n/2}+1$ such that $p \equiv q \equiv 1 \bmod k$ and $\gcd(\varphi(\ell), \varphi(m)) = k$.
(iii) Compute $k(\ell) = (p-1)p^{r-1}$ and $k(m) = (q-1)q^{s-1}$.

By Lemma 17.2(iii), Algorithm 17.7 produces the desired output. It follows from Proposition 17.5 that Algorithm 17.7 runs in polynomial time (note that the input in Algorithm 17.7 includes the group law on G).

Remark 17.8. Our prime powers ℓ and m play the roles that in the Gentry-Szydlo paper [3] were played by auxiliary prime numbers $P, P' > 2^{(n+1)/2}$ such that $\gcd(P-1, P'-1) = 2n$. Our $k(\ell)$ and $k(m)$ replace their $P-1$ and $P'-1$. While the Gentry-Szydlo primes P and P' are found with at best a probabilistic algorithm, we can find ℓ and m in polynomial time with a deterministic algorithm. (Further, the ring elements they work with were required to not be zero divisors modulo P, P' and other small auxiliary primes; we require no analogous condition on ℓ and m, since by Definition 9.5, when L is invertible then for *all* m, the $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$-module L/mL is free of rank 1.)

The next result will provide the proof of correctness for a key step in our main algorithm.

Lemma 17.9. *Suppose e is a short vector in an invertible G-lattice L, suppose $\ell, m \in \mathbb{Z}_{\geq 3}$, and suppose $e_{\ell m} \in L$ is such that $e_{\ell m} + \ell mL$ generates $L/\ell mL$ as a $(\mathbb{Z}/\ell m\mathbb{Z})\langle G\rangle$-module. Then $e^{k(m)}$ is the unique short vector in the coset $e_{\ell m}^{k(m)} + mL^{k(m)}$, and there is a unique $s \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$ such that $e^{k(m)} \equiv se_{\ell m}^{k(m)} \bmod \ell L^{k(m)}$. If further $b \in \mathbb{Z}_{>0}$ and $bk(m) \equiv k \bmod k(\ell)$, then e^k is the unique short vector in $s^b e_{\ell m}^k + \ell L^k$.*

Proof. Since e is short, we have $\mathbb{Z}\langle G\rangle e = L$. Thus for all $r \in \mathbb{Z}_{>0}$, the coset $e + rL$ generates L/rL as a $\mathbb{Z}\langle G\rangle/(r)$-module. We also have that $e_{\ell m} + mL$ generates L/mL as a $\mathbb{Z}\langle G\rangle/(m)$-module, and $e_{\ell m} + \ell L$ generates $L/\ell L$ as a $\mathbb{Z}\langle G\rangle/(\ell)$-module. Thus, there exist $y_m \in (\mathbb{Z}\langle G\rangle/(m))^*$ and $y_\ell \in (\mathbb{Z}\langle G\rangle/(\ell))^*$ such that $e_{\ell m} = y_m e \bmod mL$ and $e_{\ell m} = y_\ell e \bmod \ell L$. It follows that $e_{\ell m}^{k(m)} \equiv e^{k(m)} \bmod mL^{k(m)}$ and $e_{\ell m}^{k(\ell)} \equiv e^{k(\ell)} \bmod \ell L^{k(\ell)}$.

We have $(\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle e = L/\ell L = (\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle e_{\ell m}$. Thus

$$(\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle \cdot e^{k(m)} = L^{k(m)}/\ell L^{k(m)} = (\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle \cdot e_{\ell m}^{k(m)},$$

so

$$e^{k(m)} \equiv s e_{\ell m}^{k(m)} \mod \ell L^{k(m)} \tag{17.10}$$

for a unique $s \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$. We have $e \cdot \bar{e} = 1$, so $e \in \Lambda^*$ and $e + \ell\Lambda \in (\Lambda/\ell\Lambda)^*$. By (17.10) we have $(e + \ell\Lambda)^{k(m)} = s(e_{\ell m} + \ell\Lambda)^{k(m)}$ in $\Lambda/\ell\Lambda = \bigoplus_{i\in\mathbb{Z}} L^i/\ell L^i$. It follows that $e_{\ell m} + \ell\Lambda \in (\Lambda/\ell\Lambda)^*$.

If $ak(\ell) + bk(m) = k$ with $a \in \mathbb{Z}$, then $e^k = (e^{k(\ell)})^a (e^{k(m)})^b \equiv (e_{\ell m}^{k(\ell)})^a (s e_{\ell m}^{k(m)})^b \equiv s^b e_{\ell m}^k \bmod \ell\Lambda$, so $s^b e_{\ell m}^k + \ell L^k$ contains the short vector e^k of L^k. In both cases, uniqueness follows from Proposition 4.1. □

18. The main algorithm

We present the main algorithm. That it is correct and runs in polynomial time follows from the results above; see the discussion after the algorithm. As before, k is the exponent of the group G and $k(j)$ is the exponent of $(\mathbb{Z}\langle G\rangle/(j))^*$ if $j \in \mathbb{Z}_{>0}$.

Algorithm 18.1. Given G, u, and a G-lattice L, the algorithm determines whether there exists a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$, and if so, computes one.

(i) Apply Algorithm 10.2 to check whether L is invertible. If it is not, terminate with "no".
(ii) Apply Algorithm 17.7 to produce prime powers ℓ and m as well as $k(\ell)$ and $k(m)$.
(iii) Use Proposition 10.1 to compute $e_{\ell m}$.
(iv) Use Algorithm 14.8 to compute the pair $(L^{k(m)}, e_{\ell m}^{k(m)} + \ell m L^{k(m)})$. Use Algorithm 4.2 to decide whether the coset $e_{\ell m}^{k(m)} + mL^{k(m)}$ contains a short vector $\nu_m \in L^{k(m)}$, and if so, compute it. Terminate with "no" if none exists.
(v) Compute $s \in (\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle$ such that $\nu_m = s e_{\ell m}^{k(m)} + \ell L^{k(m)}$ in $L^{k(m)}/\ell L^{k(m)}$.
(vi) Use the extended Euclidean algorithm to find $b \in \mathbb{Z}_{>0}$ such that $bk(m) \equiv k \bmod k(\ell)$.
(vii) Use Algorithm 14.6 to compute the lattices $L^2, L^3, \ldots, L^k$ as well as data for the multiplication maps $L \times L^i \to L^{i+1}$ (for $1 \le i < k$). Also compute $e_{\ell m}^k + \ell L^k \in L^k/\ell L^k$.

(viii) Compute $s^b \in (\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle$, and compute $s^b e_{\ell m}^k \in L^k/\ell L^k$. Use Algorithm 4.2 to decide whether the coset $s^b e_{\ell m}^k + \ell L^k$ contains a short vector $\nu \in L^k$, and if so, compute it. Terminate with "no" if none exists.

(ix) Apply Algorithm 16.4 to find $e \in L$ such that $\nu = e^k$ and $e \cdot \bar{e} = 1$ (or to prove there is no G-isomorphism), and let the map $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ send x to xe.

Remark 18.2. Note that we do not use Algorithm 14.8 to compute L^k. This is because Algorithm 16.4 requires more information about L^k than is provided by Algorithm 14.8, namely, the information needed for the construction of the order A.

Proposition 18.3. *Algorithm 18.1 is a deterministic polynomial-time algorithm that, given a finite abelian group G, an element $u \in G$ of order 2, and a G-lattice L, outputs a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ or a proof that none exists.*

Proof. By Theorem 12.4(iii), the G-lattice L is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if L is invertible and has a short vector. Algorithm 10.2 checks whether L is invertible. If it is, we look for an $e \in L$ such that $e\bar{e} = 1$.

Algorithm 17.7 produces prime powers $\ell, m \geq 2^{n/2}+1$ such that $\gcd(k(\ell), k(m)) = k$. The algorithm in Proposition 10.1 produces $e_{\ell m}$, which then serves as both e_m and e_ℓ. Algorithm 4.2 finds a short vector ν_m (if it exists) in the coset $e_{\ell m} + mL^{k(m)} \in L^{k(m)}/mL^{k(m)}$. If $e \in L$ is short, then $\nu_m = e^{k(m)}$ by Lemma 17.9. Algorithm 4.2 produces a short ν in the coset $s^b e_{\ell m}^k + \ell L^k$ or proves that none exists. By Lemma 17.9, if $e \in L$ is short then $\nu = e^k$. Algorithm 16.4 then finds a short vector $e \in L$, or proves that none exists. The map $x \mapsto xe$ gives the desired G-isomorphism from $\mathbb{Z}\langle G\rangle$ to L. □

Remark 18.4. There is a version of the algorithm in which checking invertibility in step (i) is skipped. In this case, the algorithm may misbehave at other points, indicating that L is not invertible and thus not G-isomorphic to $\mathbb{Z}\langle G\rangle$ by Lemma 9.6. At the end one would check whether $\langle e, e\rangle = 1$ and $\langle e, \sigma e\rangle = 0$ for all $\sigma \neq 1, u$. If so, then $\{\sigma e\}_{\sigma\in S}$ is an orthonormal basis for L, and $x \mapsto xe$ gives the desired isomorphism; if not, no such isomorphism exists.

Thanks to Corollary 14.3, we can convert Algorithm 18.1 to an algorithm to test whether two G-lattices are G-isomorphic (and produce an isomorphism).

Algorithm 18.5. Given G, u, and two invertible G-lattices L and M, the algorithm determines whether there is a G-isomorphism $M \xrightarrow{\sim} L$, and if so, computes one.

(i) Compute $L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}$.

(ii) Apply Algorithm 18.1 to find a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}$, or a proof that none exists. In the latter case, terminate with "no".

(iii) Using this map and the map $\overline{M} \otimes_{\mathbb{Z}\langle G\rangle} M \to \mathbb{Z}\langle G\rangle$, $\overline{y} \otimes x \mapsto \overline{y} \cdot x$, output the composition of the (natural) maps

$$M \xrightarrow{\sim} \mathbb{Z}\langle G\rangle \otimes_{\mathbb{Z}\langle G\rangle} M \xrightarrow{\sim} L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M} \otimes_{\mathbb{Z}\langle G\rangle} M \xrightarrow{\sim} L \otimes_{\mathbb{Z}\langle G\rangle} \mathbb{Z}\langle G\rangle \xrightarrow{\sim} L.$$

References

[1] N. Bourbaki, Eléments de mathématique. Algèbre. Chapitres 4 à 7, Springer, Berlin, 2007.

[2] N. Bourbaki, Elements of mathematics. Commutative algebra, Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972.

[3] C. Gentry and M. Szydlo, *Cryptanalysis of the revised NTRU signature scheme*, Advances in Cryptology—EUROCRYPT 2002, Lect. Notes in Comp. Sci. **2332**, Springer, Berlin, 2002, 299-320, full version at `http://www.szydlo.com/ntru-revised-full02.pdf`.

[4] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), 265–338.

[5] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[6] H. W. Lenstra, Jr., *Lattices*, in Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press, Cambridge, 2008, 127–181.

[7] H. W. Lenstra, Jr. and A. Silverberg, *Revisiting the Gentry-Szydlo Algorithm*, in Advances in Cryptology—CRYPTO 2014, Lect. Notes in Comp. Sci. **8616**, Springer, Berlin, 2014, 280–296.

[8] H. W. Lenstra, Jr. and A. Silverberg, *Determining cyclicity of finite modules*, submitted.

[9] H. W. Lenstra, Jr. and A. Silverberg, *Roots of unity in orders*, in preparation.

Mathematisch Instituut, Universiteit Leiden, The Netherlands
E-mail address: `hwl@math.leidenuniv.nl`

Department of Mathematics, University of California, Irvine, CA 92697, USA
E-mail address: `asilverb@uci.edu`

List of Symbols, Abbreviations, and Acronyms

FHE Fully Homomorphic Encryption

LLL Lenstra-Lenstra-Lovász lattice basis reduction algorithm

$\mathbb{Z}$ the integers

$\mathbb{Z}[X]$ the set of polynomials in one variable X with integer coefficients

$|G|$ the number of elements in a set G